VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Průzkum řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na VŠ

Survey on Risk Control and Management Resulting from Security Threats at University

Student: Bc. Andrea Owczarzová

Vedoucí diplomové práce: doc. Ing. Milena Tvrdíková, CSc.

Ostrava 2015

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Andrea Owczarzová**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 6209T025 Systémové inženýrství a informatika

Téma: Průzkum řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na VŠ
Survey on Risk Control and Management Resulting from Security Threats at the University

Zásady pro vypracování:

1. Úvod
2. Řízení a zvládání rizik v mobilním a cloudovém prostředí
3. Analýza současného stavu řízení rizik na VŠ
4. Vyhodnocení průzkumu
5. Návrh doporučení pro zvládání rizik na VŠ
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

DOUCEK, Petr a kol. *Řízení bezpečnosti informací*. 2. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.
ONDRÁK, Viktor, Petr SLÁDEK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. 377 s. ISBN 978-80-7204-872-4.
RHODES-OUSLEY, Mark. *Network Security: the Complete Reference*. 2nd ed. New York: McGraw Hill, 2012. 896 p. ISBN 978-007-1784-351.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Milena Tvrdíková, CSc.**

Datum zadání: 21.11.2014
Datum odevzdání: 25.04.2015

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA OSTRAVA Ekonomická fakulta 1

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Místopřísežné prohlášení o samostatném vypracování diplomové práce.

„Prohlašuji, že jsem celou práci, včetně všech příloh, vypracovala samostatně“.

Touto formou bych ráda poděkovala doc. Ing. Mileně Tvrdíkové, CSc. a Ing. Michalu Slámovi za poskytnutí mnoha podnětných rad, které mi pomohly k vypracování této práce.

V Ostravě dne 25. 4. 2015

Bc. Andrea Owczarzová

Obsah

1 Úvod

Informační bezpečnost je vzhledem ke stále rostoucím hodnotám informací, čím dál více frekventovanějším pojmem. Bezpečnost informací je problém řešený, jak v komerční tak i státní sféře. Jen myšlenka či pocit firmy nebo státní instituce o ztrátě, změně či odcizení důležitých dat, pro každodenní chod společnosti, je nemyslitelná. Proto je nutné se proti potencionálním hrozbám bránit.

Internetové útoky nejsou jen útoky specialistů, kteří jdou cíleně za informacemi. Z takových to cílených útoků se stávají dobře promyšlené obchody. Avšak kromě cílených útoků, jsou známé i útoky lidí, kteří si dokazují pouze své možnosti, znalosti a dovednosti.

Kromě cílených útoků, za účelem, kterým jsou firmy a státní instituce vystavovány, existují i útoky na jednotlivce. Málokdo si dokáže připustit, že internet je sám o sobě nebezpečný. Člověk na internetu tráví nezanedbatelnou část jak pracovní doby, tak svého volného času a málokdo si uvědomuje, kolik osobních dat a informací na internetu sdílí. Proto má bezpečnostní politika a řízení a zvládání rizik v dnešní době velký význam.

Pro studenty a zaměstnance vysokoškolského, či jiného školního sektoru, je v dnešní době internetové prostředí velmi významné. Existují podpůrné systémy pro vzdělávání, informace o studentech jsou ukládány v elektronické podobě, na vysokých školách se již nepoužívá index (výkaz o studiu). Informace o prospěchu studentů jsou ukládány v digitální podobě. Studenti čím dál více využívají cloud computingových služeb pro sdílení dokumentů, které mají jako skupina vypracovat. Tyto technologie mají stále větší využití a jsou označovány za moderní. Bohužel existují lidé, kteří chtějí získat informaci o studentech, školním systému či informaci o profesorech. Napadení jakoukoliv podobou je velmi nebezpečné a je nutné se bránit.

Proto se tato práce zejména věnuje řízení a zvládání rizik v cloud computingovém a mobilním prostředí na vysokých školách. Téma bezpečnosti je popsáno ve druhé kapitole, která pojednává i o cloud computingu (dále jen „CC“) a mobilním prostředí.

O CC se v současné době mluví poměrně často, hlavně z důvodů využití CC v malých a středních firmách, zařazování CC do výuky studentů a stále větším využití u běžných uživatelů v domácnostech.

Sám pojem cloud computing je lidem znám, avšak význam tohoto pojmu je nejednoznačný. Pomocí několika definic je pojem cloud computing v práci popsán, další část práce je věnována samotné bezpečnosti při použití cloud computingových technologií.

CC má své zastánce i odpůrce, jedním z odpůrce je Richard Stallman, zakladatel projektu GNU (GNU's Not Unix). Pan Stallman právě poukazuje především na nebezpečí ztráty soukromí uživatelů a nárůst moci společností, u kterých jsou data uživatelů ukládaná.

Cílem práce je na základě teoretických poznatků a pojmů, jako je CC, IT služba a virtualizace, zabývat se možností jejich využití ve vysokoškolském informačním systému. Práce se zaměřuje na legislativu, možnosti rizik v CC, následně pak na opatření týkajících se bezpečnosti a zvládání rizik v IS/ICT. Třetí kapitola je věnována přiblížení průzkumů, které jsou použity k analýze stavu řízení a zvládání rizik na veřejných vysokých školách z pohledu studentů a z pohledu veřejných vysokých škol. Následně na tuto kapitolu navazuje kapitola čtvrtá, která se zabývá průzkumy a vyhodnocením těchto průzkumů. Podle výsledku průzkumu stavu řízení a zvládání rizik na vysokých školách jsou navržena doporučení pro zvládání těchto rizik.

2 Řízení a zvládání rizik v mobilním a cloudovém prostředí

Tato část je věnována problematice cloud computingu a mobilnímu prostředí, následně je pak vymezena problematika řízení a zvládání rizik.

Velmi úzce je s CC spjata technologie virtualizace. Dny, kdy byly vztahy mezi hardwarem a operačním systémem one-to-one, už minuly. Virtualizace umožňuje, aby na jednom fyzickém serveru běželo více oddělených serverů s vlastním operačním systémem, tuto funkci zajišťuje hypervisor. Hypervisor je mezivrstva, která dovoluje spustit na jednom fyzickém počítači více nezávislých virtuálních strojů.

Virtualizace vytváří zajímavou bezpečnostní výzvu, jelikož většina bezpečnostních rizik pochází ze zneužití softwaru. Ve virtualizovaném prostředí je téměř vše software.

Hypervisor zodpovídá za řízení všech zařízení, která hostují na fyzickém serveru viruálního stroje. Centralizované prostředí poskytuje Service Console, ta je zodpovědná za správu všech serverů ve virtuálním prostředí. Kompromis hypervisora a Service Console je přijatelný, avšak přináší nebezpečí snížení bezpečnosti dat, potencionálně by mohl způsobit značné škody v bezpečnosti, kdy by se všechny bezpečnostní kontroly vynechaly.

Hypervisor a Service Console musí být řádně zajištěny a opravovány, stejně tak musí být logicky odděleny pomocí izolovaných sítí s přísnými kontrolami vstupů. Administrativní rozhraní by mělo být umístěno na síti, odděleno od virtuálních strojů a jiných aplikačních serverů. Firewall by měl být použit k blokování přístupu z virtuálních strojů na konzoli pro správu. Toto nastavení chrání před útoky a dopady malware na virtuální stroj.

2.1 Cloud computing

Cloud computing je poměrně mladá a rozvíjející se technologie, jak již bylo zmíněno, tento pojem je vysvětlován různě. Proto existuje mnoho definic CC, výběr z nich je uveden níže.

První z uvedených říká, že cloud computing neboli sdílení hardwarových i softwarových prostředků pomocí sítě je na internetu založený model vývoje a používání počítačových technologií. Lze ho také charakterizovat jako poskytování služeb či programů uložených na serverech na internetu s tím, že uživatelé k nim mohou přistupovat například pomocí internetového prohlížeče nebo klienta dané aplikace a použít je prakticky odkudkoliv. (Ondrák, Sedlák a Mazálek, 2013, str. 242)

Zítko definuje pojem cloud computing pomocí překladu z anglického do českého jazyka. Uvádí, že cloud je oblak a computing znamená výpočetní, po spojení těchto slov dostaneme tedy výpočetní oblak. Výpočetní oblak je pak definován, jako veškeré služby online nebo přes internet. Výpočetní výkony se provádějí v oblaku, jímž je právě internet. Zítko říká, že často se cloud computing definuje jako datové uložiště. (Zítko, 2013)

Další uvádí, že cloud computing přichází s myšlenkou většího zaměření na samotný cíl využití IT infrastruktury a software, než na jeho technickou realizaci. Infrastrukturu, vývojovou a aplikační platformu i software, převádí proto do formy služby. Tuto službu poskytuje svým zákazníkům poskytovatel cloud computingu obvykle prostřednictvím internetu nebo jiné vysokorychlostní datové sítě. (Zikmund, 2010)

Gary Breder, jenž je ředitelem globálního marketingu EMC a na prostředí cloud computingu se specializuje, definoval cloud computing takto: „Cloud computing je metoda přístupu využití výpočetní techniky, která je založena na poskytování sdílených výpočetních prostředků a jejich využívání formou služby. Existují nejrůznější modely služeb a možnosti jejich poskytování. Pro všechny typy cloud computingu je společná schopnost poskytovat prostředky na vyžádání, elasticky, samoobslužně a prostřednictvím přístupu z rozsáhlé sítě a také schopnost měřit spotřebované služby v rámci sdíleného fondu prostředků.“ (Cloud.cz)

Poslední definici, která je uvedena, je definice Marka Rhodes-Ousleyho. Ten říká, že cloud computing poskytuje způsob, jak zvýšit kapacitu nebo přidat funkce za chodu bez investování do nové infrastruktury, školení nových zaměstnanců nebo kupování licence na nový software. Uživatel si tedy vybere služby a platí jen za ty, které používá. Tento způsob rozšiřuje možnosti využití IT. (Rhodes-Ousley, 2012, str. 578)

2.2 Vývoj cloud computingu

CC se začal vyvíjet již před padesáti lety, kdy John McCarthy, jenž je považován za otce myšlenky CC, jako první prezentoval myšlenku sídlení počítačových technologií. John McCarthy, profesor na americké univerzitě MIT, tuto myšlenku prezentoval v roce 1961, mimo jiné tento profesor přišel s termínem AI (Artificial Intelligence) – umělá inteligence.

John McCarthy v roce 1961 prohlásil, že jednoho dne budou výpočetní prostředky dostupné jako veřejná služba, podobně jak je tomu například u distribuce elektrické energie, zemního plynu nebo vody.

Robert Metcalfe, spoluvynálezce Ethernetu, formuloval pravidlo, které popisuje působení síťového efektu, který je platný v médiích i technologiích. Užitečnost sítě (dokonce i sítě sociální) roste se čtvercem počtu připojených uzlů – uživatelů nebo zařízení. Metcalfe definoval vztah mezi počtem uživatelů a přínosem technologie. Pokud nové technologie používá mnoho lidí, jen tehdy jsou užitečné. Jinými slovy, čím více lidí používá produkt nebo službu, standart či software, tím je síť cennější a přitahuje další uživatele. Užitek sítě je dán čtvercem počtu uživatelů a na křivce existuje bod, od kterého pak již roste užitek exponenciálně. (Pavlíček, 2010)

Termín „cloud computing“ se objevil až v roce 1997. Tento pojem použil na své přednášce Ramnath Chellap. Pojem cloud je chápán jako oblak. Oblak používaný v telekomunikacích, znázorňuje připojení koncových stanic k internetu. Tento oblak byl dříve nazýván utility computingem, dnes je již nazýván cloud computingem.

V roce 2006 vznikla první komerční služba CC – Amazon Web Services (AWS). O rok později se k Amazon Web Services připojily firmy Google a IBM (International Business Machines). V roce 2007 začala řada univerzit pracovat na vědeckých a komerčních programech založených na CC.

Od roku 2009 je CC vnímán jako klíčová budoucí technologie, mezi své nejdůležitější technologie ji zařadily i firmy jako HP (Hewlett Packard) i Microsoft. V témže roce firma Microsoft zveřejnila beta verzi Windows Azure. V roce 2010 byl zahájen komerční provoz Windows Azure. Nejrozšířenějším příkladem CC je webmail, například Gmail od společnosti Google, českou alternativou je email.cz.

CC má tři klíčové charakteristiky. První charakteristikou je dostupnost služby. Stačí se jen zaregistrovat, případně rovnou zaplatit. Druhou charakteristikou je škálovatelnost,

což znamená, že kapacita může být dynamicky a skokově měněna. Třetí charakteristikou je vysoká míra samoobslužnosti.

2.3 Dělení cloud computingu

Termín cloud computing je pro uživatele matoucí a mnoho uživatelů by právě s cloud computingovou technologií chtělo pracovat. Různé využití je jedním z důvodu existence více typů služeb pod značkou cloud services. Uvedené typy jsou nejčastěji používané a jsou rozdělené podle způsobu, jak je cloud computing nasazován anebo podle toho, jakou službu CC poskytuje.

2.3.1 Modely nasazení cloud computingu

Tento typ rozdělení říká, jak je cloud computing poskytován. Poskytování může být veřejné, soukromé, hybridní a komunitní.

Veřejný (Public Cloud Computing) nebo také klasický model CC. S tímto typem CC se setkala většina uživatelů, i přesto, že si to uživatelé neuvědomují. Je to služba, která je poskytována a nabídnuta široké veřejnosti. Uživatelé internetu již běžně používají pokročilé e-mailové schránky, webové kalendáře. Veřejný CC poskytuje stejnou nebo velmi podobnou funkcionalitu všem uživatelům, příkladem jsou Google Apps, Skype nebo seznam.cz či datová uložiště jako ulozto.cz a edisk.cz.

Privátní (Private Cloud Computing) je v tomto případě provozován pouze pro jednu konkrétní firmu, společnost, organizaci či korporaci. Nerozlišuje se, zda CC provozuje organizace samotná nebo se o pronájem stará třetí společnost. Tento typ CC je vytvářen speciálně pro organizaci, takzvaně „na míru“.

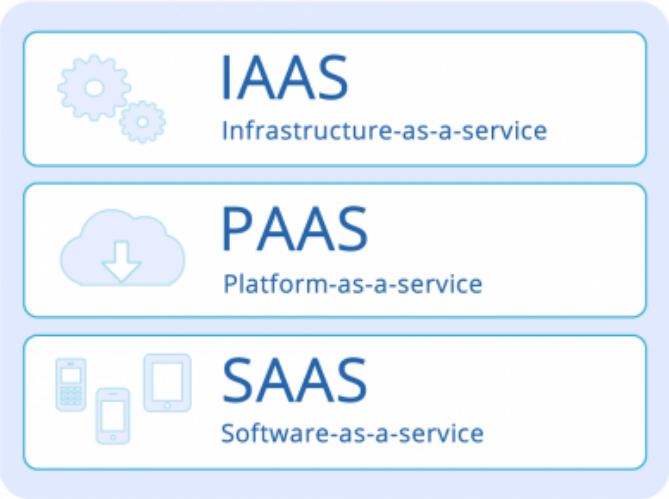
Komunitní (Comunity Cloud Computing) je model, kdy je infrastruktura cloud computingu sdílená mezi více organizacemi nebo skupinou lidí. Tyto organizace nebo skupiny lidí může spojovat bezpečnostní politika nebo stejný obor zájmu.

Hybridní (Hybrid cloud computing) CC kombinuje jak veřejné, tak soukromé cloud computingy. Může kombinovat i různé typy CC. Hybridní CC navenek vystupuje jako jeden cloud computing. Cloud computingy jsou propojeny pomocí standardizačních technologií. Přístupy hybridního CC se v příštích letech stanou významnou hnací silou rozvoje IT v obchodním prostředí. (Zive.cz, 2011)

2.3.2 Distribuční modely cloud computingu

Tyto typy rozdělení jsou založeny na tom, co je v rámci služby nabízeno. Společným označením pro distribuční rozdělení je dodatek „as a Service“. Tento dodatek pak používají typy, na které se distribuční rozdělení dělí, například „IaaS“, „SaaS“, „PaaS“. První písmeno typu cloud computingu, pak značí konkrétní druh poskytované služby – Infrastructure as a Service, Software as a Service a Platform as a Service.

Na obrázku č. 2.1 jsou zobrazeny tři hlavní služby distribuované v cloud computingu.



Obr. 2.1 Rozdělení podle distribučního modelu (zdroj: arcusglobal.com)[1]

SaaS je využití softwaru jako služby. U tohoto modelu distribuce si zákazník nekupuje software, ale pronajímá si ho. Výhodou je tedy, že klient nebo zákazník si nemusí software kupovat či instalovat. Dále pak poskytovatel může snížit cenu na základě množstevní výhody, popřípadě se o software starat a aktualizovat ho. Využití tohoto distribučního modelu je levnější. Typickými aplikacemi SaaS jsou e-mail nebo CRM (Customer Relationship Management) systémy a další.

PaaS znamená, že platforma je služba. U této služby si uživatel pronajímá platformu, která bude hostovat jeho aplikaci. Tento přístup je známý pro vývojáře. Aplikace, která bude vytvořena, bude nahrána na server. Dalo by se říci, že tento přístup je podobný hostingu. Avšak u PaaS se platí spotřebované megackly procesoru za hodinu, nevýhodou je malý výběr prostředí a velká závislost na poskytovateli. Příkladem mohou být Google App Engine či GigaSpaces.

[1] http://www.arcusglobal.com/assets/IAAS-400x300.png

IaaS využívá infrastrukturu jako službu. To znamená, že uživatel si pronajme počítač, na který bude nahrán operační systém, dle uživatelova výběru. Následně uživatel platí, za hodiny, kdy je počítač využíván. Výhodou této služby je, že uživatel se nemusí starat o údržbu a provoz hardwaru. Příkladem IaaS je Amazon Web Services či Windows Azure od společnosti Microsoft.

2.4 Výhody a nevýhody cloud computingu

Náklady na služby jsou jedna z mnoha výhod CC. Zákazník nemusí znát princip fungování počítače či operačního systému. CC umožňuje sdílení jak hardwaru, tak softwaru. Sdílení prostředků, jako jsou hardware a software, znamená menší ekonomické náklady. Jedinými náklady zde budou investiční výdaje, které zahrnují přechod na cloud computingové služby a následně licence za klientský software, pokud je placený.

Flexibilita je nejsilnější výhodou. Zákazník může měnit odebírané množství velmi pružně a tomu odpovídá i cena právě využívaných služeb. Zákazník platí pouze za to, co v dané chvíli využívá. Důležitá je schopnost systému dynamicky měnit počty uživatelů, kteří mohou využívat software a také alokovat hardwarové zdroje. Zákazník může kdykoliv požádat o přidání operační paměti, výkonu procesoru nebo navýšit objem datového úložiště.

Nezávislost na platformě, mobilita a dostupnost služeb, k datovému centu se může uživatel připojit odkudkoliv. Cloud computing poskytuje nezávislost na platformě. Například SaaS aplikace distribuují skrz tenkého klienta, kterým je v naprosté většině webový prohlížeč. Standardem je dostupnost služeb z 99,95% s dopředu plánovanými výpadky kvůli údržbě.

Automatické aktualizace patří mezi výhody, poskytovatel se stará o aktuálnost aplikací pro zákazníka. I když jsou změny hlášeny předem, tak s sebou přinášejí jistá rizika. Automatický update může způsobit změny, které nejsou vítány, proto je důležité, aby téma aktualizací bylo podrobně popsáno ve smlouvě s poskytovatelem.

Ochrana dat, ohledně bezpečnosti dat mezi uživateli panuje nejvíce obav. Poskytovatelé cloud computingových služeb si nemohou dovolit jakoukoliv ztrátu dat. Při ztrátě dat by mohli přijít jak o postiženého zákazníka a ztrátu důvěryhodnosti, tak i o potencionální zákazníky. Při problému se ztrátou dat je na tom spotřebitel dnes lépe, jelikož se může bránit využitím obchodního zákoníku.

Menší ekologická zátěž se taktéž řadí mezi výhody.

Cloud computing jako „buzzword“, cloud computing je relativně novým pojmem v IT. Z toho důvodu existují názory, jako například názor pana Richarda Stallmana, který říká, že CC je pouze marketingovou kampaní. U CC neexistuje skoro žádné dlouhodobé spolehlivé doporučení ohledně používání této technologie.

Závislost na poskytovatelích je jednou z nevýhod CC. Poskytovatel si může diktovat podmínky, proto hrozí například případné zdražení služeb.

Bezpečnost dat a legislativa, cloud computing je kritizován obhájci soukromí. Těmto lidem se nelíbí to, že poskytovatel CC má kontrolu nad osobními údaji. Kromě sledování osobních údajů mohou poskytovatelé sledovat i komunikaci. Bezpečnost služeb je proto spornou otázkou, avšak vznikly již právní kontroly a předpisy. Zastánci cloud computingu se domnívají, že data o zákaznících jsou chráněna dostatečně. Poskytovatelé mají silnou motivaci k udržení důvěry. Zákazník i poskytovatel se musí řídit právním řádem, avšak nastává problém, kdy se poskytovatel může řídit jinou jurisdikcí a zákazník také. Příkladem jsou společnosti, které sídli v USA, nebo poskytují službu z USA. Tyto společnosti jsou ze zákona povinné postoupit data klienta vládě v souladu s Patriot Actem, což ale může kolidovat s povinnostmi ochrany osobních údajů klienta. (Ondrák, Sedlák a Mazálek, 2013, str. 243)

2.5 Přínosy cloud computingu při použití ve vzdělávání

Server www.veskole.cz zveřejnil článek, který se zabývá přínosy cloud computingu ve vzdělávání. Cloud computing přináší flexibilitu práce s uloženými daty a umožňuje především formu komunikace. Zabývá se použitím tabletů a aplikací při výuce. Je zmíněn snadný přístup, například webovým prohlížečem, k uloženým datům a jednoduché, uživatelsky přívětivé, ovládání prostředí cloud computingu. Jedním z největších přínosů pro studenty je sdílení dokumentů, přednášek či jiného výukového materiálu. Je zmíněna i spolupráce studentů nad jedním dokumentem. Dále je vyzdvihnut problém, kdy je student nemocný a pedagog může pomocí CC technologie s takovýmto studentem komunikovat, popřípadě mu distribuovat učivo. Tento typ výuky je velmi účinným, jelikož on-line uložiště umožňují uložení jakéhokoliv multimediálního obsahu, který je pro studenty zajímavější, názornější a více atraktivnější. Změny v multimediálních souborech probíhají okamžitě na všech zařízeních. Dalším přínosem je využití pro profesory a pedagogy, kdy si CC službou mohou zjednodušit administrativu a správu rozvrhu, klasifikaci a absenci žáků. (Loužecká, 2015)

Dalšími kladnými přínosy využívání CC služeb ve výuce jsou možnost výuky potřebného množství studentů, kapacita studentů lze flexibilně měnit v čase, přístup k aplikaci z jakéhokoliv místa, podpora týmové práce, pedagog má kontrolu nad přístupem studentů ke studiu. CC aplikace nezatěžují univerzitní servery. (Tvrdíková, 2013)

2.6 Řízení a zvládání rizik

Tato část se věnuje základním pojmům, jako je bezpečnost informací a charakteristice bezpečnosti. Jsou zde vysvětleny termíny jako integrita dat, dostupnost a důvěrnost.

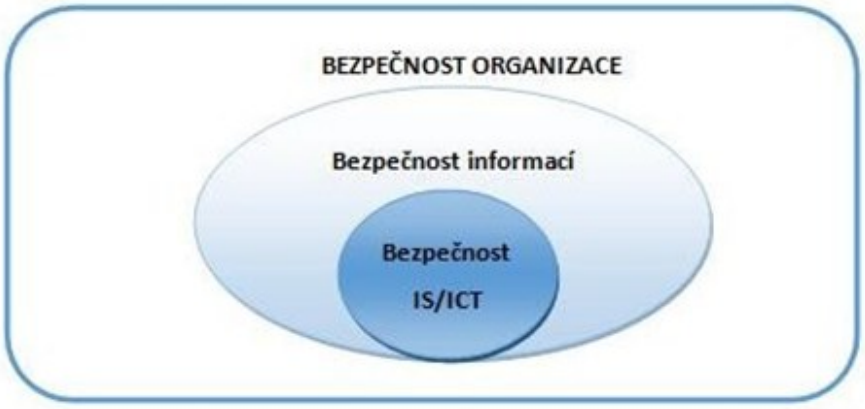
Informace nemusí mít pouze podobu elektronickou, mohou mít podobu i písemnou či dokonce podobu myšlenky. Těmito informacemi jsou utajované výrobní postupy, různé receptury či znalost přístupových hesel. Pokud je informace ve formě myšlenky, tak je poměrně těžké zajistit její bezpečnost. Bezpečnost této informace závisí zcela na majiteli a jeho důvěře. Avšak existují prostředky, kterými lze riziko snížit.

Doucek a kolektiv (2011, str. 56) tvrdí, že v souvislosti s bezpečností informací je nutno zmínit dva pojmy a těmi jsou bezpečnost organizace a bezpečnost IS/ICT. Pod pojmem bezpečnost organizace je chápáno především zajištění fyzické bezpečnosti. Fyzická bezpečnost může například znamenat instalace kamerového systému, biometrického systému či ostraha objektu, která bude vykonávaná specializovanou firmou. Fyzická bezpečnost pomáhá zajistit bezpečnosti IS/ICT.

Bezpečnost IS/ICT chrání výhradně aktiva, která jsou součástí informačního systému organizace, tedy aktiva nehmotná. Obrázek č. 2.2 zobrazuje rozdělení bezpečnosti organizace, bezpečnosti informací a bezpečnosti IS/ICT.

Nejvyšší kategorií je bezpečnost ogranizace. Součástí bezpečnosti organizace je zajištění bezpečnosti objektů, majetku orgnaizace, jako je ostraha přístupů do objektů, strážní služba atd. Její součástí, kromě jiných, je i bezpečnost informací. Cílem a úkolem řízení bezpečnosti informací je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů. Bezpečnost IS/ICT má za úkol chránit aktiva, která jsou součástí informačního systému firmy, podporovaného informačními a komunikačními technologiemi.

(Doucek a kolektiv, 2011, str. 56)



Obr. 2.2 Bezpečnost organizace (zdroj: autor)

Bezpečnost informací musí splňovat tři základní předpoklady. Informace musí být dostupná, tedy musí být zajištěno to, že informace a s ní spojená aktiva jsou uživatelům přístupná v době, ve které je požadují. Druhým předpokladem je důvěrnost, což znamená, že informace je přístupná pouze oprávněnému uživateli. Posledním předpokladem bezpečnosti informace je integrita. Integrita je zajištění správnosti a úplnosti informace.

Dalšími důležitými pojmy jsou aktivum, které vymezuje veškerý hmotný a nehmotný majetek, a hrozba, jenž je událost ohrožující bezpečnost. (Ondrák, Sedlák a Mazálek, 2013, str. 15)

K ustanovením ISMS, neboli Information Security Management Systém, patří řízení rizik, hodnocení rizik, vyhodnocení a zvládání rizik. Jednotlivé kroky jsou popsány níže.

Řízení rizik (Risk Management) je koordinace potřebná k řízení a kontrole organizace s ohledem na rizika. Hodnocení rizik (Risk Assessment) je proces analyzování a vyhodnocování rizik. Analýzou rizik (Risk Analysis) je systematické používání informací pro odhad míry rizika a určení jeho zdrojů. Vyhodnocení rizika (Risk Evaluation) je proces porovnávání odhadnutého rizika s danými kritérii pro určení jeho významu. Zvládání rizik (Risk Treatment) je proces výběru a přijímání opatření pro snížení rizika. Akceptace rizika (Risk Acceptance) je rozhodnutí přijmout riziko. Prohlášení o aplikovatelnosti (Statement of Aplicability) je dokument s popisem opatření v ISMS organizaci.

(Ondrák, Sedlák a Mazálek, 2013, str. 16)

2.6.1 Informační bezpečnost

V této části kapitoly jsou, pro správné pochopení problematiky informační bezpečnosti, popsány hrozby pro informační bezpečnost a následně pak normy a zákony. Prvním důležitým pojmem je riziko.

Riziko je kombinací pravděpodobnosti události (hrozby) společně s jejím dopadem. Jedná se o ztrátu, poškození či zničení aktiva. Míra rizika se vypočte pomocí vzorce, kde se s hrozbou sečte zranitelnost a dopad na aktivum. (Ondrák, Sedlák a Mazálek, 2013, str. 17)

Hrozba je událost, která může vyvolat incident, jenž může způsobit poškození systému nebo organizace. Hrozba využívá zranitelnosti k získání či poškození aktiva. Hrozby se rozdělují na tři skupiny – přírodní a fyzické, technické a technologické a lidské. Přírodní a fyzické jsou pohromy, které mohou být živelného charakteru, požáry, povodně, vichřice, ale i nehody, jako například porucha v dodávce elektrického proudu. Technické a technologické jsou poruchy technologických komponent IS/ICT, jako například porucha nosičů dat. Dále to mohou být poruchy sítí či poruchy způsobené nefunkčností programů, ke kterým se řadí i viry a trojské koně. Lidské hrozby se dělí na dvě podskupiny neúmyslné a úmyslné. Neúmyslné hrozby jsou provedeny lidmi bez zlého úmyslu, jsou způsobeny nedostatečnou kvalifikací, neznalostí nebo dokonce nedbalostí. Úmyslné hrozby se dělí na hrozby z okolí systému – hackeři, teroristé nebo mezifiremní špióni, a hrozby zevnitř – zlomyslní a ziskuchtiví zaměstnanci či návštěvníci organizace.

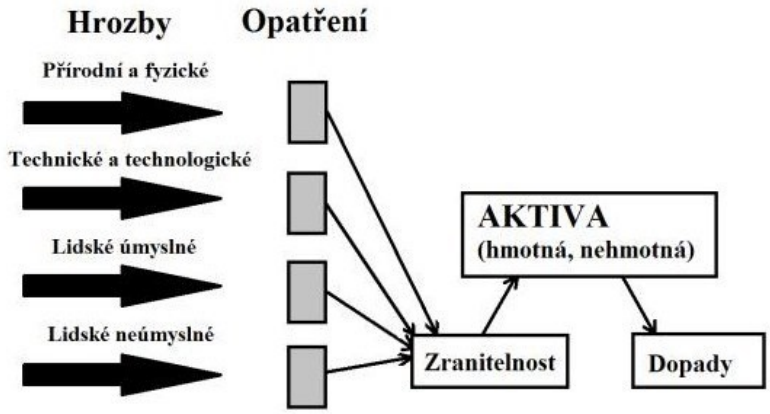
Většina hrozeb, které poškodí IS/ICT organizace spadají mezi lidské neúmyslné. Taktéž podíl ohrožení zevnitř organizace je vyšší než ohrožení organizace zvenčí. Doucek a kolektiv (2011, str. 58) říká, že podle některých statistických zdrojů je až 98% bezpečnostních incidentů v organizaci interního původu. Nejčastěji se mezi tyto incidenty řadí právě nedbalost pracovníků, která je nejčastěji způsobená jejich neodbornou kvalifikací či neznalostí problematiky IS/ICT.

Hrozby se dělí na neoprávněné, náhodné nebo úmyslné:

- prozrazení interních informací organizace, kdy dojde k prozrazení dat,
- upravení, dojde k porušení integrity dat,
- zničení,
- bránění v dostupnosti dat, zdrojů nebo služeb informačního systému autorizovaným uživatelům.

(Doucek a kolektiv, 2011, str. 58)

Podle Chlupa patří mezi nejčastější hrozby selhání dodávky energie, škodlivý software, selhání hardwaru a selhání komunikačních služeb.



Obr. 2.3 Koncept zajištění bezpečnosti ve firmě (zdroj: Doucek a kolektiv, str. 57)

Obrázek č. 2.3 zobrazuje koncept zajištění bezpečnosti IS/ICT ve firmě. Jsou zde zobrazeny vztahy mezi aktivy a hrozbami a jak tyto hrozby mohou na aktiva působit. Je zobrazena i možná zranitelnost a dopady hrozeb na aktiva, dále pak ochrana aktiv formou opatření.

Aktivem je cokoliv, co má vypovídající hodnotu pro organizaci – informace, majetek i osoby. Mezi osoby se řadí zaměstnanci a zákazníci. Majetkem jsou chápany všechny hmotné a nehmotné statky. Mezi hmotná aktiva patří výpočetní technika – počítače, kabelové rozvody, tiskárny a ostatní technická zařízení. Nehmotná aktiva se dělí na pracovní postupy, data, programové vybavení a služby. (Doucek a kolektiv, 2011, str. 56)

Zranitelnost je slabé místo aktiva, které může být využito v rámci určité hrozby. Jedná se o slabinu nebo mezeru v bezpečnosti, která by mohla být využita v rámci získání neautorizovaného přístupu k aktivu. Zranitelnost je rozdělována na fyzickou, zranitelnost

technických a programových prostředků – nosičů dat, elektromagnetických zařízení, komunikačních systémů a kabelových rozvodů či personální.

Opatření znamená řízení rizik včetně politik, směrnic, postupů nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy. Opatření umožňují snížit sílu hrozby, která na informační systém působí nebo úplně zabránit v jejím účinku. Opatření je rozdělováno podle charakteru – administrativní opatření, fyzické opatření, technické a technologické opatření.

Opatření je rozděleno i podle cílů, které sledují – prevenční, detekční, korekční. Prevenční cíl zajišťuje minimalizaci rizik. Detekční cíl odhaluje potencionální problémy a hrozby. Korekční cíl zajišťuje minimalizaci dopadů poté, co hrozba nastala a projevila se.

Analýza rizik slouží k odhadu ztrát, které mohou vzniknout působením hrozeb a dává přehled o stupni nebezpečnosti jednotlivých hrozeb, slabých místech a rizicích, které na podnik působí.

2.6.2 Požadavky ochrany pro informační bezpečnost

Existuje řada definic informačního systému, jelikož každý uživatel či tvůrce informačního systému používá různé terminologie a zdůrazňuje jiné aspekty informačního systému. Informační systém lze také definovat, jako soubor technologických prostředků, osob, procesů a metod, které zabezpečují sběr, zpracování, přenos a uchování informací pro využití v rámci organizace.(Šmíd)

Informační systém je možno rozdělit na tři hlavní části, jimiž jsou hardware, software a komunikace. Toto rozdělení pak umožní lépe identifikovat a aplikovat postupy ochrany a prevence, které jsou zahrnuté v normách o informační bezpečnosti na třech úrovních organizace – personální úroveň, fyzická úroveň a organizační úroveň.

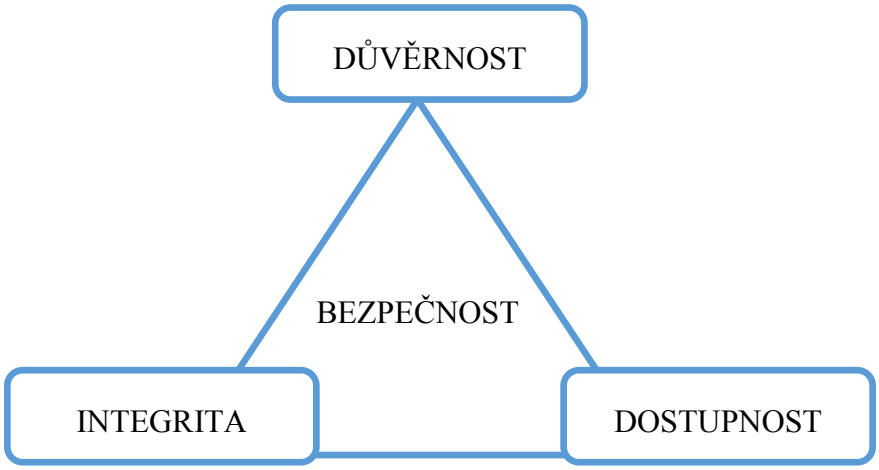
Informační bezpečnost má za úkol ochraňovat výše zmíněné informace proti neautorizovanému přístupu, odposlechu, modifikaci, zničení a dalším činnostem. Počítačová bezpečnost má základní trojici bezpečnostních cílů – důvěrnost, integritu a dostupnost. Tato trojice se nazývá CIA triad. CIA triáda je zobrazena na obrázku č. 2.4

Důvěrnost znamená, že zdroje nebo informace jsou utajené. Tato potřeba utajovat informace vzniká z důvodu používání počítačů v oblastech jako je státní správa, školství, armáda či nemocnice. Informace v těchto sektorech musí být utajované. Mezi tyto oblasti spadá i průmysl, kde si firmy chrání zdrojový kód či design před konkurenčními firmami.

Podle normy ČNS ISO/IEC 27000:2009 je důvěryhodnost vlastnost, která činí informací nedostupnou či neodhalitelnou neautorizovaným jednotlivcům, entitám nebo procesům.

Integrita se vztahuje na integritu dat a na integritu originality. Integrita originality je označována jako autenticita, to znamená, že data musí být správná a úplná. Podle normy ČNS ISO/IEC 27000:2009 je integrita zajištění správnosti a úplnosti informací.

Dostupnost vypovídá o zajištění přístupu k informacím nebo prostředkům ve stanovenou dobu (nebo do stanovené doby). Mezi nejznámější pokusy o zamezení dostupnosti přístupu k datům nebo službám se nazývají DoS útoky (Denial of Service attacks). Podle normy ČNS ISO/IEC 27000:2009 je dostupnost vlastnost přístupnosti a použitelnosti na žádost autorizované entity.



Obr. 2.4 Trojice CIA v organizaci (zdroj: autor)

2.6.3 Legislativa a normy

Je představena aktuálně používaná legislativa a aktuálně používané normy, které se zabývají informační bezpečností v právním prostředí České republiky, určené pro práci s informačními technologiemi a informační bezpečností.

Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti (zákon č.412/2005 Sb.) v právním prostředí České republiky upravuje zásady pro stanovení informací, jako informací utajovaných. Zákon stanovuje podmínky pro přístup k utajovaným informacím a další požadavky na jejich ochranu. Dále zákon stanovuje zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb.) je v souladu s právem Evropské unie, mezinárodními smlouvami, kterými je Česká republika vázána.

Zákon stanovuje práva a povinnosti při zpracování osobních údajů, dále pak podmínky, za nichž se uskutečňují předávky osobních údajů do jiných států.

Tento zákon se zabývá osobními údaji, citlivými údaji, kde pro zajímavost patří i biometrické a genetické údaje.

Zákon stanovuje povinnosti informační bezpečnosti pro organizace spravující a zpracovávající osobní údaje. Organizace musí pomocí opatření zabránit neoprávněnému přístupu, změně, zničení, ztrátě či odcizení osobních údajů. Musí také zabránit neoprávněnému přenosu, zpracování a jinému zneužití těchto údajů.

Zákon o elektronickém podpisu (zákon č. 227/2000 Sb.) se zabývá použitím elektronického podpisu, který je nástrojem autentizace a identifikace právnických a fyzických osob v prostředí informační společnosti. Zákon vymezuje dva způsoby pro označení elektronického dokumentu fyzickou osobou, a těmi jsou Elektronický podpis a Zaručený elektronický podpis. Následně tento zákon vymezuje povinnosti podepisující osoby, povinnosti kvalifikovaného poskytovatele certifikačních služeb a postihy při případném neplnění povinností.

Zákon o informačních systémech veřejné zprávy (zákon č. 365/2000 Sb.) ve svém úplném znění určuje práva a povinnosti vztahující se k tvorbě, provozování, rozvoji a užívání informačních systémů veřejné správy. Tento zákon také používá mírně odlišnou definici informačního systému. Informačním systémem se tak pro účely tohoto zákona rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost.

Normy ISO/IEC 27000 jsou mezinárodně platným standardem, který definuje pravidla pro systémy řízení bezpečnosti informací (ISMS – Information Security Management System). Normy vycházejí z konceptu modelu PDCA (Plan-Do-Check-Act), jenž je zobrazen na obrázku č. 2.5.

Obr. 2.5 PDCA (zdroj: www.system2win.com)[2]

Klíčovou normou je norma ISO/IEC 27001:2005, která se zabývá právě systémem řízení bezpečností informací a jeho požadavky. Tato norma vychází z normy britského standartu BS 7799-2, který byl vydán v říjnu 2005.

Další důležitou normou je norma ISO/IEC 27002, jenž se nazývá Soubor postupů pro řízení bezpečnosti informací a skládá se ze 133 bezpečnostních opatření.

ISO/IEC 27006 se zabývá požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti, tato norma upřesňuje pravidla pro udělování certifikací ISMS.

Existuje mnoho dalších norem a i připravovaných norem, mezi které se řadí ISO/IEC 27017. Tato norma se bude zabývat poskytováním doporučení pro zabezpečení cloud computingu. Norma ISO/IEC 27018 se bude zabývat poskytováním doporučení ohledně ochrany osobních údajů v CC.

[2] http://www.systems2win.com/LK/lean/PDCA.png

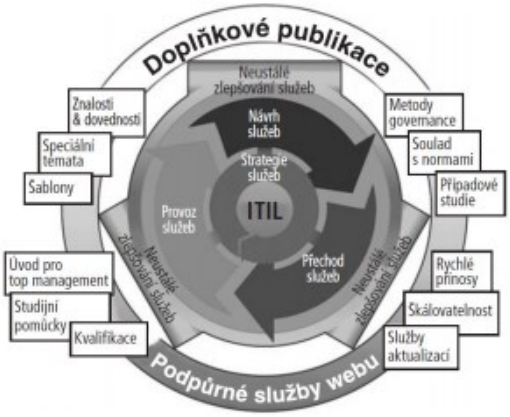
Framework ITIL (Information Technology Infrastructure Library) představuje rámec (nikoli metodiku), který obsahuje popis způsobů procesního řízení služeb včetně infrastruktury IT. ITIL se koncentruje na plánování, vytváření, modifikaci, dodávku, správu, analýzu a použití služeb.

Knihovnu ITIL spravuje organizace Office of Government Commerce a je šířená formou knih, školení, konzultací a certifikací. ITIL je v současnosti již mezinárodním standardem pro oblast řízení IT služeb.

ITIL V3 (verze 3) vypracovaná v květnu 2007 se skládá z pěti základních titulů definujících strategii, návrh, přechod, provoz a neustálé zlepšování služby.

Verze 3 je zobrazena na obrázku č. 2.6.

Strategie služeb (Service Strategy) je základem rámce ITIL, představuje propojení aktivit organizace se strategií v oblasti informatiky – informační strategie. Návrh služeb (Service Design) obsahuje návrh služeb IT a architektury informačního systému v organizaci, v celém životním cyklu, včetně různých forem sourcingu a sdílených služeb. Implementace služeb (Service Transition) zahrnuje návody na implementaci služeb do reálného prostředí. Zahrnuje procesy jako například řízení změn, řízení verzí, modely služeb, návrh kontrol pro uvádění služeb do provozu. Provoz služeb (Service Operation) podporuje správu služeb v produktivním prostředí, řešení problémů, poruch, stanovení ukazatelů jakosti služeb a podobně. Průběžné zlepšování služeb (Continual Service Improvement) pomáhá zlepšovat zavedené existující služby. (Doucek a kolektiv, 2011, str. 50)



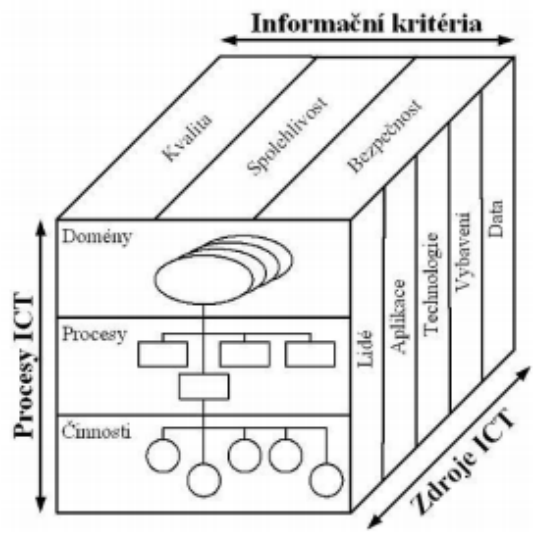
Obr. 2.6 Základní model ITIL (zdroj: Doucek a kolektiv, str. 49)

ITIL samotný však neřeší problém bezpečnosti technologií, pouze představuje nejdůležitější aktivity. Je doporučené použití i specializovaných postupů, jako rodiny ISO/IEC 27000.

Framework CobiT (Control Objectives for Information and related Technology) je framework pevně spjat s organizací ISACA (Information Systems Audit and Control Foundation), jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, které mají za cíl pomoci organizacím maximalizovat užitek plynoucí z informačních technologií.

V současné době je COBIT ve verzi páté, která vyšla v 1. čtvrtletí roku 2012.

Základní princip COBIT je založen na cílech organizace, zdrojích informačních technologií a procesech. Tyto tři komponenty využívá takzvaná COBIT kostka, která je zobrazena na obrázku č. 2.7.



Obr. 2.7 Kostka COBIT (zdroj: Bukovský, 2008)[3]

COBIT kostka přehledně znázorňuje vzájemné prolínání procesů IT (na úrovni domény, procesů a činností), zdrojů ICT a požadavků na informační kritéria (efektivnost, výkonnost, důvěrnost, integrita, dostupnost, shoda, hodnověrnost). Z COBIT kostky je zřetelné, že jsou definovány různé úrovně podrobnosti. Nejobecnější jsou definice domén. Ty COBIT specifikuje čtyři – plánování a organizace, akvizice a implementace, dodávka a podpora, sledování a hodnocení.

[3] http://deathless.cz/documents/COBIT.pdf

COBIT obsahuje 34 procesů, které pokrývají oblast byznysu a informačních technologií. Některé procesy mají obecný vztah k bezpečnosti informačních technologií, jako je PO9 – Posuzování a správa IT rizik z domény plánovaní a organizace. Kontrolní body COBIT se přímo vztahují k informační bezpečnosti, tímto bodem je například bod DS5 – Zabezpečení systémové bezpečnosti. V tomto dokumentu jsou definovány následující oblasti: management bezpečnosti informačních technologií, plán informační bezpečnosti, správa identit uživatelů, správa uživatelských účtů, monitoring, dohled a testování informační bezpečnosti, definice bezpečnostních incidentů, ochrana bezpečnostních technologií, management šifrovacích klíčů, prevence, detekce a náprava škodlivého software, bezpečnost počítačové sítě a výměna citlivých utajovaných informací. (Knotek)

2.6.4 Práce s utajovanými informacemi

Práce s utajovanými informacemi se řídí legislativou danou zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti (zákon č. 412/2005 Sb.). Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Způsoby zajištění bezpečnosti informací se dělí na oddíly – personální bezpečnost, průmyslová bezpečnost, fyzická bezpečnost, bezpečnost informačních a komunikačních systémů a kryptografická ochrana.

Personální bezpečnost se zabývá fyzickými osobami, které přistupují k citlivým informacím, v akademickém prostředí to jsou profesoři, pedagogové, ale taktéž pracovníci studijního oddělení. Například taktéž lidé, kteří se zabývají stipendii. Úroveň utajení se dělí na přísně tajnou, tajnou a důvěrnou, kdy v zákoně jsou popsané možné ohrožení či dopady při úniku takové citlivé informace.

Průmyslová bezpečnost nastavuje systém opatření, který dovoluje zajišťovat a ověřovat dodržování podmínek pro přístup organizace k citlivým informacím a práci s nimi. Organizace, v tomto případě akademické prostředí, musí být schopna řádně zabezpečit citlivé informace, nejen o studentech, proti odcizení či zneužití. Organizace by měla mít ustanovenou zodpovědnou osobu.

V případě, kdy organizace potřebuje ke své činnosti pracovat s citlivými daty, musí splňovat předpoklady pro získání takzvaného Osvědčení podnikatele pro práci s utajovanými informacemi od NBÚ (Národní bezpečnostní úřad). Toto osvědčení lze udělit pouze

organizaci, která je ekonomicky stabilní, bezpečnostně spolehlivá a je schopna zajistit zabezpečení citlivých informací.

Fyzická bezpečnost se zabývá ochranou informací v rámci ochrany objektů a jejich zabezpečením. Je pravidlem tyto objekty kontrolovat pomocí ostrahy, režimových opatření či technických prostředků.

Bezpečnost informačních a komunikačních systémů se zabývá definicí souborem postupů a opatření pro zajištění bezpečnosti citlivých informací v těchto systémech. Komunikační systém je definován jako systém zajišťující přenos citlivých informací mezi koncovými uživateli a komunikačním zařízením, takovýmto systém lze například nazvat systém Vysoké školy báňské – Technické univerzity Ostrava EDISON (Education Information Systém on Net), který je zároveň systémem informačním.

Pro zajištění jakýchkoliv hrozeb je důležité a nutné informační systém chránit a je taktéž nutné provést analýzu rizik. Bezpečnost informačního systému musí být zajišťována, dle vyhlášky č. 523/2005 Sb. O bezpečnosti informačních a komunikačních systémech a dalších elektronických zařízeních nakládajících s utajovanými informacemi a o certifikaci[4], současně v šesti oblastech: počítačová a komunikační bezpečnost, kryptografická ochrana, ochrana proti úniku kompromitujícího vyzařování, administrativní bezpečnost a organizační opatření, personální bezpečnost a fyzická bezpečnost IS.

Na informační systém obsahující citlivé informace, tudíž i na výše zmiňovaný EDISON, jsou stanoveny minimální požadavky dle vyhlášky č 523/2005 Sb., které musí systém splňovat:

- identifikace a autentizace všech uživatelů před přístupem k informačnímu systému,
- zajištění důvěrnosti a integrity autentizační informace,
- volitelné řízení přístupu k objektům IS,
- zajištění nemožnosti získat informace z paměti objektu po ukončení práce s ním,
- záznam událostí v IS potenciálně ovlivňujících bezpečnost a jejich uchování pro audit,
- možnost auditu a vyvození odpovědnosti všech uživatelů,
- zabezpečení integrity auditních informací a ochrana před zničením,

[4]http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005/

- zajištění důvěrnosti informace během přenosu.

Kryptografická ochrana zajišťuje přímou ochranu citlivých informací pomocí užití kryptografických metod při jejich zpracování, přenosu a ukládání.

2.6.5 Konkrétní oblasti opatření cloud computingu

a) Administrativní opatření

Správa identit, role a práva, zaměstnanci by měli mít přístup jen k datům, které potřebují k výkonu své práce, jinak hrozí potencionální zneužití či manipulace se softwarem, ať už z nedbalosti nebo cíleně za účelem.

O proniknutí do IT systémů mohou usilovat i jedinci z vně organizace, výsledek je vždy katastrofální. Pro regulaci neoprávněného přístupu, je třeba ochraňovat programy, regulovat přístup k přístrojům, softwaru či datům. Opatřením by mohla být digitální identita pro zaměstnance a systémy založené na rolích. CC služby mají zdvojený bezpečnostní mechanismus. Nejprve kontrolují přístup k CC samotnému, potom ke cloud computingové službě. Zde je v návaznosti na zdvojený přístup nutná také zdvojená autentizace. (Lejsek, 2013)

Infrastruktura firmy a bezpečná komunikace v cloud computingu, základním rysem cloud computingových služeb je, že při přenosu dat mezi uživatelem a poskytovatelem nejsou data vystavena ohrožení i přesto, že přenos probíhá veřejnou sítí.

Při přenosu dat veřejnými sítěmi, například internetem, je nutností data šifrovat. Profesionální poskytovatelé nabízejí standardizované nebo speciální zákaznické služby jako PKI (Public Key Infrastructure), které umožňují bezpečný, ověřený a šifrovaný přenos dat.

Pro přístup ke službám CC ve firemní síti (intranet nebo LAN) musí být rovněž implementovaná ochranná opatření (firewall a systémy detekce průniku).

V případě síťových komunikačních služeb poskytovaných dodavatelem, je nutné aplikovat integrované mechanismy pro oddělení datových toků, které jsou zasílané různým uživatelům a službám. (Lejsek, 2013)

IT v datových centrech, při používání cloud computingového řešení nesmí mít uživatel přístup k datům jiného uživatele. Pokud by to bylo možné, pak by počítačoví zločinci mohli instalovat špionážní software či jiný malware s účelem ohrozit všechny uživatele, kteří využívají daného CC řešení.

Pro oddělení systému se používají lokální sítě VLAN (Virtual Local Area Networks) a firewally, jenž brání uživateli v přístupu k serverům, aplikacím a datům jiného uživatele.

Data jsou v CC izolována v oblastech, tak aby uživatelé měli přístup pouze ke svým datům. (Lejsek, 2013)

Bezpečná komunikace a správa služeb, v souvislosti s CC je důležitá zeměpisná poloha zpracování a ukládání dat. Právní prostředí nemusí být stejné v zemi, kde firma sídlí a v zemi, ze které je CC poskytován. Firmy by se měly orientovat v regionálních zákonech, ohledně dodržování soukromí v zemi, ve které poskytovatel CC sídlí. Regulatorní rámec vyžaduje, aby byly podniky schopny uvést, ve které zemi jsou jejich data uložena. Daňové zákony v Evropské unii a jiných zemích například dovolují finančním orgánům přístup k informacím, které jsou relevantní pro daňové účely.

Jsou-li cloud computingové služby poskládány do komplexní nabídky, není dodávka vždy snadnou záležitostí. I když jsou aplikace distribuovány, musí jednotlivé složky cloud computingové služby vykazovat efektivní součinnost aby byl zajištěn spolehlivý provoz. Složitější cloud computingové nabídky často zahrnují služby třetí strany. V kontraktu, je proto nutné jasně specifikovat, jaké služby budou kým dodávány. Popřípadě kdo nese právní odpovědnost v případě jakýchkoli otázek. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

Ochrana systému u poskytovatele služeb, poskytovatelé služeb disponují firewallovými systémy, které však nemají zabudovanou funkčnost ochrany proti průniku, proto nemohou zajistit dostatečný stupeň ochrany. Efektivní ochranu síťových segmentů tvoří firewally kontrolující komunikaci, porty, aplikace a firewally k hloubkové kontrole a dále pak skenující protokoly o přenosu dat.

Dalšími klíčovými mechanismy jsou proxy servery a reverzní proxy. Tyto mechanismy filtrují a přeměňují příchozí a odchozí datový provoz, chrání citlivé informace, minimalizují zranitelná místa a přispívají k větší bezpečnosti ICT. (Lejsek, 2013)

b) Fyzické opatření

Fyzické zabezpečení datového centra, data centra jsou aktiva a musí být taktéž chráněná. Možnosti ochrany mohou být prostředky fyzických mechanismů a přístupových kontrol.

Datacentra musí být postavená tak, aby budova odolala přírodním katastrofám, potencionální fyzické sabotáži a ohni. Zařízení musí být vzdáleno od oblastí s výskytem bouří, záplav a zemětřesení. Kromě toho musí být zajištěno dobré dopravní spojení, dodávky vody a elektřiny. Po celé budově musí být prováděny kontroly přístupu a zvláště citlivá data musí být ukládána ve speciálně oddělených oblastech. (Lejsek, 2013)

Organizace bezpečnosti a bezpečná administrace, lidský faktor hraje v bezpečnosti cloud computingových služeb hlavní úlohu. Poskytovatelé provozují systém informační bezpečnosti (ISMS - Information Security Management Systém), který definuje procesy a pravidla, poskytující referenční model a nástroje pro plánování, implementaci, ověřování a úpravy informační bezpečnosti.

Klíčovou roli hrají privilegovaná práva administrátora. Správci mají obvykle zvláštní práva, která musí být pečlivě řízena. Řízení práv pak zajišťuje dostatečnou bezpečnost, blokací přístupů a znemožnění provádění určitých funkcí.

Nedílnou součástí těchto infrastruktur je monitorování bezpečnostních událostí a záznamů dat. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

Správa služby a dostupnost, poskytovatelé CC zajišťují dostupnost vytvářením zálohovacích systémů pro jednotlivé aplikace. Pro posílení dostupnosti poskytovatelé taktéž využívají zdvojování datových center. Poskytovatel garantuje požadovanou úroveň dostupnosti tím, že používá odpovídající archivační systémy. Efektivní správa služeb zajišťuje, aby byly plněny všechny potřeby zákazníka a aby byly prováděny jakékoliv nutné změny.

Součástí této služby jsou spolehlivé procesy ITIL, jako řízení změn, problémů a releasů. Existuje mnoho otázek souvisejících s ICT, které uživatelské organizace nedokážou řešit samy. Proto potřebují přístup ke zkušenostem poskytovatele služby s ohledem na probíhající údržbu a vývoj systémů a služeb. Někteří poskytovatelé nabízejí zákazníkům také čtyřiadvacetihodinovou správu dodávky služby, kdykoli poskytují dodatečnou podporu. Zjistí-li zákazníci pokles dostupnosti nebo dojde k narušení bezpečnosti či k jinému problému, mohou kontaktovat svého manažera dodávky služeb a požádat o podniknutí patřičného opatření. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

c) Technické a technologické opatření

Kontrakty, integrace procesů a migrace. Určení, zda začlenění cloud computingových služeb ovlivní projekty nebo vytvoří bezpečnostní rizika, závisí výrazně na tom, zda existují informace o možnostech spolupráce mezi poskytovatelem a zákazníkem. V některých případech je rovněž třeba splnit specifické firemní bezpečnostní požadavky. Externě dodávané ICT služby podléhají vnitřním předpisům zákazníka. Poskytovatelé ICT používají systém řízení bezpečnosti, který definuje požadavky, implementuje a sleduje všechny nutné změny. Když poskytovatel například zjistí, že do zákazníkova systému pronikl útočník, spolupracuje s uživatelskou organizací při hledání nejlepšího řešení.

Bezpečnost může kladně ovlivňovat také přizpůsobivost. Outsourcingové modely například zjednodušují počet bezpečnostních úkolů ICT, protože jsou služby dodávány centrálně odborníky. Tyto služby zahrnují implementaci, konfiguraci, aktualizaci, zálohování, monitoring a údržbu. Podniky mohou určovat úroveň bezpečnosti, kterou potřebují. Služby se dodávají na modulární základně „plať podle potřeby“ a jsou jasně definovány ve smlouvě o úrovni služeb (SLA). Před jejím podpisem by poskytovatel i zákazník měli společně zjistit, jaké aplikace mají kritický význam a co se stane v případě poruchy. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

Řízení bezpečnosti a zranitelnosti, složky ICT, složky ICT infrastruktury občas vykazují chyby či slabiny. Dochází k nim kvůli programátorským chybám nebo špatnému nastavení. Často se objevují při změnách požadavků a scénářů nasazení. Aby se předcházelo větším problémům, musí být tyto slabiny odhalovány a včas řešeny.

Tento složitý proces zahrnuje analýzu různých informačních zdrojů. Cloud computingová datová centra musí být ověřena podle mezinárodně uznávaných norem jako ISO/IEC 2700 a shoda musí být pravidelně ověřována nezávislými auditory. Norma ISO 27001 vyžaduje, aby poskytovatelé používali systém řízení bezpečnosti informací (ISMS), který zahrnuje řízení bezpečnosti a rizik a rozsáhlý bezpečnostní rámec. ISMS je klíčovým řídicím nástrojem k dosažení a udržování požadovaného stupně bezpečnosti. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

Vykazování bezpečnosti a řízení událostí, události související s bezpečností jsou součástí každodenního provozu ICT. Jejich analýza umožňuje úpravu, náhradu nebo zdokonalování opatření. Nápravu je třeba podnikat v závislosti na tom, do jaké míry určitá událost porušila bezpečnostní postupy. Zákazník musí být informován, aby mohl provést

odpovídající změny. Firma může být za jistých okolností nucena odpovídat na dotazy sdělovacích prostředků nebo poskytovat vysvětlení svým zaměstnancům a zákazníkům. Proto je důležité začlenit procesy, jako záznam dat, řízení, sledování, analýzu, podchycování, vyhodnocování a řízení bezpečnostních událostí do provozu ICT. Uživatelské organizace vyžadují přehled o tom, jak poskytovatel cloud computingové služby řídí. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

Řízení požadavků a shoda, firmy musí splňovat zákonné, regulační a specifické odvětvové požadavky. Zahrnuje to i vnitřní postupy, kontrakty se zákazníky, dodavateli, partnery a další závazky, s nimiž vyslovily souhlas. Žádné dvě organizace nejsou stejné. Liší se svými procesy a potenciálními hrozbami. Dále pak ve stupni negativního vlivu bezpečnostních událostí na byznys. Mají však jedno společné – potřebují silného partnera, který nabízí bezpečnou a zajištěnou cestu CC. Technická infrastruktura obvykle existuje. Avšak její spojení se specifickým byznysem firmy vyžaduje péči a v některých případech čas. (Lejsek, 2013), (Ondrák, Sedlák a Mazálek, 2013, str. 245)

2.7 Základní požadavky ochrany informační bezpečnosti v cloud computingu

Při řešení cloud computingových služeb se musí řešit bezpečnost. Objevují se různé druhy hrozeb, jelikož data mohou být uložena v soukromých i veřejných CC datových centrech. Při použití tolika platforem se pořád objevují nové hrozby. Dle Marka Rhodes-Ousleyho datová centra a cloud computing vyvolávají důležité otázky a obavy, které musí být řešeny.

Dostupnost, cloud computingové služby lze srovnávat s internetem. Na internetu je dostupnost hrozeb řízena používáním redundantních služeb poskytovatelů, takže porucha u poskytovatele nemá za důsledek ztráty služby.

Stálost dat, se zabývá tím, co se stane, pokud budou data z CC vymazány.

Patriot Act, tento Act je znám v USA, Americká vláda má právo sledovat a zachytit veškerý provoz poskytovatele služeb. Pokud je poskytovatel požádán o to, aby ho Americká vláda mohla sledovat a zachycovat provoz, musí to udělat bez ohledu, na to si zákazník myslí.

PCI dodržování, toto dodržování vyžaduje, aby uživatel i poskytovatel mohl prokázat, kde přesně se jejich data nachází a na co jsou fyzicky uložena.

Migrace, je možností přenesení dat formou physical-to-cloud a cloud-to-physical. Což znamená přenesení dat z počítače zákazníka do cloud computingového prostředí.

Důvěryhodnost, odpovědnost za řízení dat v prostředí CC je rozdělena mezi poskytovatele cloud computingu a zákazníka. Izolování dat je efektivní, jen jak je efektivní virtualizace technologií a CC. Data, která jsou privátní, by neměla být umístěna ve veřejném CC.

Integrita zajišťuje, aby data byla správná a úplná.

2.8 Bezpečnostní rizika v cloud computingu

Jak již bylo zmíněno, riziko je součtem hrozby, dopadu a zranitelnosti. Cloud computing je sužován mnohými bezpečnostními riziky. Cloud computingové technologie se vyznačují některými specifickými atributy a nutně podléhají potřebě hodnocení bezpečnostních rizik v oblastech jako je integrita dat, obnova nebo ochrana soukromí a v právních záležitostech. Některá rizika na sebe přebírá poskytoval cloud computingových technologií a tudíž není nutno se těmito riziky zabývat. Dodavatel odpovídá za implementaci, audit, bezpečnost, monitoring, plán potřebných kapacit, údržbu a podporu a řízení dostupnosti. (Tvrdíková, 2013)

Níže je uveden výpis některých možných rizik.

- Nejasné vlastnické struktury, odpovědnosti a první vztahy,
- nesmí být narušena dostupnost, důvěryhodnost a integrita,
- privileged user acces, což znamená zajištění přístupu a práv lidem, kteří budou s daty a v technologii CC pracovat,
- poskytovatelé by měli být podrobování auditu a měli by být schopni udržet bezpečnost dat,
- při poskytování CC přichází otázka právní legislativy, kdy zákazník musí být obeznámen s jurisdikcí země, ve které je CC poskytován,
- při používání CC se firemní data obvykle nacházejí ve sdíleném prostředí, proto je žádoucí zajistit například šifrovací protokoly, které byly navrženy a testovány profesionály,
- poskytovatel by měl vědět, co se stane s daty či službami v případě nějaké nehody, je nutné, aby poskytovatel CC byl schopen provést kompletní obnovu dat,

- firmy by měly od svých CC poskytovatelů vyžadovat podporu konkrétních typů ošetření,
- je nutné zjistit, zda poskytovatel není v ohrožení bankrotu či převzetí od jiné firmy.

(Cloud.cz)

2.9 Rizika mobilního prostředí

Vzhledem k tomu, že chytré telefonní zařízení a tablety jsou v podstatě na úrovni počítačů, jsou tato zařízení stejně citlivá na hrozby. Tyto hrozby mohou zneužít zranitelnosti operačního systému a způsobit ztrátu nebo krádež dat, změnu v nastavení, vniknutí do chráněných vnitřních sítí a podobně.

2.9.1 Hrozby pro mobilní zařízení

Malware může infikovat chytré telefony a tablety stejně jako počítače, malware vytvoří platformu, na které mohou útočníci provádět síťové útoky a krádeže dat. Ohrožená mobilní zařízení jsou nástrojem právě pro krádež dat ze sítě, zvláště pokud to není vnímáno, jako vážné ohrožení v rámci organizace.

Datové uložiště, moderní chytré telefony, fotoaparáty a tablety mají velké množství flash paměti a jsou přístupné přes rozhraní USB (Universal Serial Bus). Toto rozhraní umožňuje zloději nenápadně kopírovat soubory. Mobilní zařízení mají datová uložiště, která mohou být použita ke kradení údajů nebo dat v organizacích.

Jednoduchá hesla, stejně jako u jiných platforem, i mobilní technologie umožňují přístup k datům a zdrojům na základě prověření uživatele. Autentizace zahrnuje prověření uživatele pomocí hesla. Mobilní zařízení pak poskytuje cestu k napadení zdrojů, ke kterým má uživatel přístup.

WI-FI Hijacking, podobně jako man-in-the-middle útoky se Wi-Fi únos provádí zákeřnými útočníky pomocí bezplatných Wi-Fi hotspotů, které jsou zřízené na veřejných místech. Tyto hotspoty se nacházejí na místech, kde koncoví uživatelé očekávají bezplatné připojení – letiště, kavárny, parky a centrální oblasti. Hotspoty jsou však často monitorovány útočníky, kteří chtějí získat osobní informaci, finanční údaje a hesla.

Otevřené Hotspoty, mobilní zařízení mohou být použita jako počítače a mohou působit v bezdrátové síti. Tato síť je vytvořena a používaná pro přístup k internetu, stejně jako bezplatná Wi-Fi síť nebo Bluetooth. Útočníci v okolí se připojí pomocí hotspotu,

který je vytvořen mobilním zařízením a následně bez vědomí zakladatele této sítě, mohou zahájit útoky na síť či zařízení.

Baseband Hacking, chytré telefony a tablety mají jak síťové, tak hlasové funkce. Volání může být zachyceno útočníkem. Útočník pak může využít zranitelnosti telefonu volajícího.

Útoky taktéž mohou být na principu vestavěného mikrofonu, který odposlouchává zařízení, i když volající právě netelefonuje.

Bluetooth Snooping and Fuzzing („Šmírování a chybování skrz Bluetooth"), uživatelé při používání funkce Bluetooth mají nastaven PIN (Personal Identification Number) defaultně na hodnotu 0000 nebo 1234. Pokud má uživatel takto nastaven PIN, tak útočník může velmi jednoduše spárovat mobilní zařízení a využívat připojení či hůř zachytit data.

Kromě tohoto typu rizika existuje i riziko známé jako „fuzzing", tento útok využívá softwarové zranitelnosti. Zařízení Bluetooth zasílá neplatná data a může způsobit abnormální chování chytrého zařízení. Mezi abnormální chování je řazena eskalace práv nebo průnik dat.

2.9.2 Útoky na operační systém mobilního zařízení

Aplikace třetích stran pro mobilní zařízení jsou psány lidmi, anonymy. Tyto aplikace jsou psány v prostředí, které uživatelé nejsou schopni kontrolovat. Není přehled o procesu, životním cyklu vývoje nebo kontrole kvality. Tyto aplikace pak mohou být nahrány do „obchodu s aplikacemi" kýmkoliv. Tyto aplikace mohou být škodlivé nebo mohou úmyslně či neúmyslně „obejít" bezpečnostní zásady a normy, které byly zavedeny v rámci organizace.

Trojský kůň, stejně jako počítače mohou být aplikace chytrého zařízení či tabletu napadnuty škodlivým softwarem. Trojský kůň vypadá jako aplikace, která obsahuje skrytý kód. Tento kód může, pokud ho vlastník neobjeví, v mobilním zařízení přetrvávat. V březnu 2011 vznikla aplikace s názvem DroidDream, která detekuje Trojské koně. Jelikož existuje nespočet aplikací, v kterých byl Trojský kůň nalezen, některé tyto aplikace byly k dispozici na autorizovaném Google Play.

URL (Uniform Resource Locator)**,** útočníci využijí URL adresy a směřují uživatele na nebezpečné webové stránky.

Phishing mobilních zařízeních představuje stejné riziko jako u počítačů. Phishing používá klasickou techniku odesílání e-mailu obsahující škodlivou přílohu či webový odkaz,

spolu s některými falešnými, ale realisticky vypadajícími zprávami za cílem oklamat koncového uživatele nebo k nepřímému donucení otevření odkazu či přílohy. Tato technika se snaží ukrást osobní informace, jako jsou čísla bankovních účtů a čísla kreditních karet.

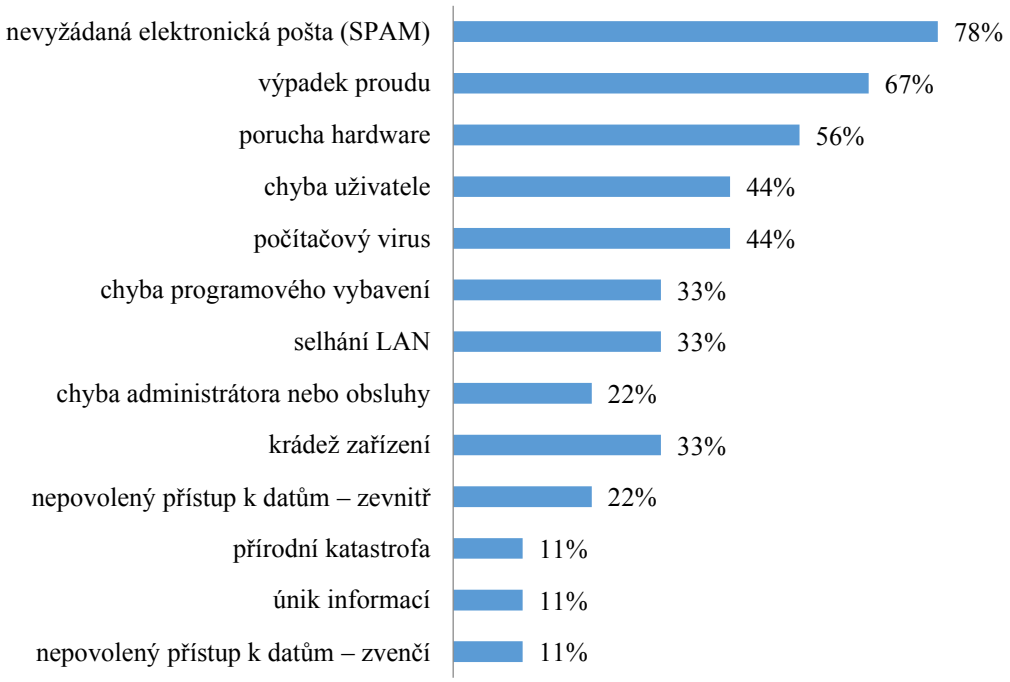
Smishing je podobné Phishingu, avšak Smishing používá textové zprávy zvané SMS (Short Message Service). Přes tyto SMS, například útočník naláká nic netušícího koncového uživatele na zavolání čísla. Tyto textové zprávy vypadají realisticky a většinou se skládají z žádosti o potvrzení nějaké informace, například z bezpečnostních důvodů nebo potvrzení nákupu, vrácení platby a tak dále.

WarTexting, zajímavým poznatkem či aplikačním rizikem, je propojení mobilních zařízení s moderními automobily. V důsledku toho mohou útoky na telefon vzdáleně spustit, sledovat nebo provozovat vozidlo.

2.10 Hrozby ve vysokoškolském systému

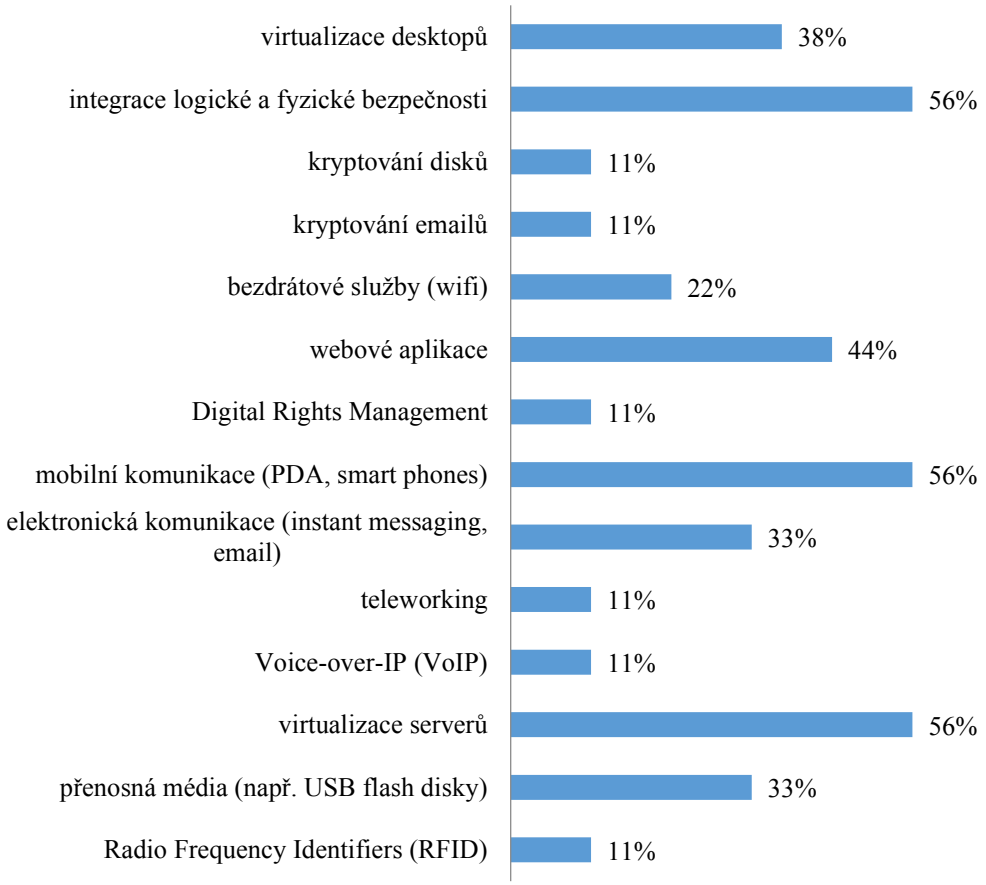
Pro zobrazení hrozeb, které mohou ve vysokoškolském systému nastat, jsou použity výsledky Průzkumu stavu informační bezpečnosti na veřejných vysokých školách v České republice za rok 2012. Tento dokument vznikl za podpory Studentské grantové soutěže na Ekonomické fakultě, VŠB-TU Ostrava.

Průzkum přinesl zajímavé výsledky týkající se například toho, jakým hrozbám čelí vysoké školy či univerzity v České republice. Všechny grafy jsou z výše zmiňovaného průzkumu.



Graf 2.1 Bezpečnostní incidenty (zdroj: PSIB)

Graf č. 2.1 zobrazuje hrozby, se kterými se veřejné vysoké školy musely potýkat. Nejčastějšími odpověďmi byly nevyžádaná elektronická pošta, výpadek proudu či porucha hardware. Lze vidět, že s nepovoleným přístupem k datům, jak zevnitř tak zvenčí se potýkalo 33% respondentů.



Graf 2.2 Výzvy z hlediska bezpečnosti (zdroj: PSIB)

Graf č. 2.2 zobrazuje, seznam bezpečnostních výzev pro vysoké veřejné školy, kde největšími výzvami jsou virtualizace serverů, mobilní komunikace a integrace logické a fyzické bezpečnosti.

2.11 Systém řízení bezpečnosti informací

V dnešním globalizovaném světě, je systém řízení bezpečnosti informací (Information Security Management System – ISMS) nedílnou součástí pro organizace. Bezpečnost je součástí řízení a vnitřní kultury. Jelikož v neustále více propojujícím světě čelí informace a práce s nimi v informačních systémech organizací seznamu bezpečnostních hrozeb. Mezi tyto hrozby patří špionáž, podvody, útoky, vandalismus a podobné.

Systém řízení bezpečnosti informací je část celkového systému řízení organizace, která je založena na přístupu (organizace) k rizikům činností, která jsou zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.

Hlavními důvody pro řízení bezpečnosti informací jsou ty, že informace jsou hodnotným aktivem. Systém řízení bezpečnosti informací snižuje míru rizika konkurence či dokonce vzniku konkurence, dalším důvodem je ochrana soukromí a cenných dat a následně budování dobrého jména organizace a důvěryhodnosti.

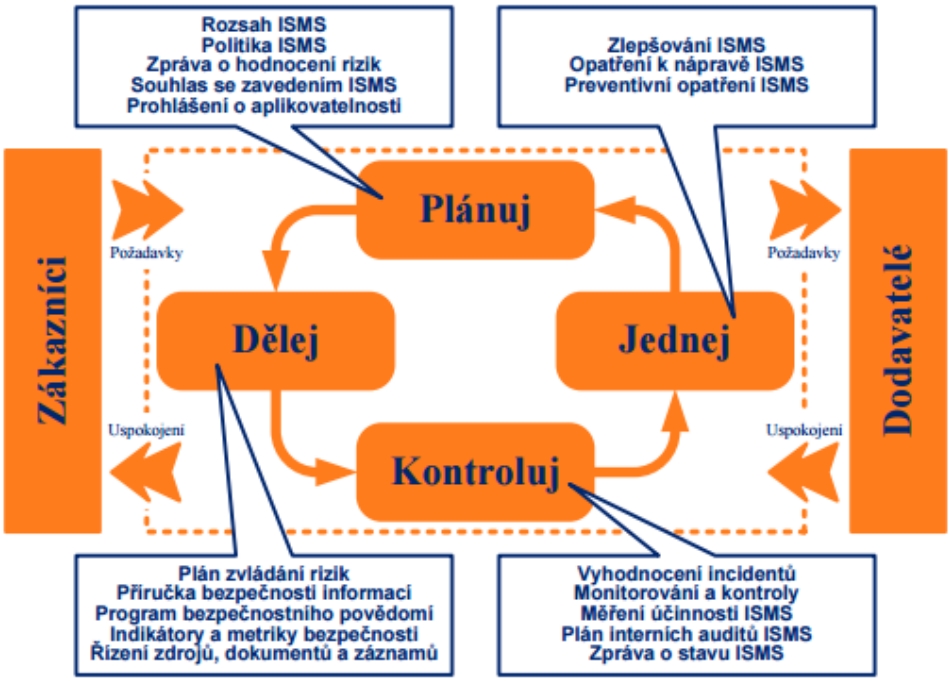
ISMS je založen na využití PDCA modelu a má čtyři etapy, které zahrnují ustanovení ISMS (určuje rozsah a zodpovědnosti), zavádění a provoz ISMS (prosazení vybraných bezpečnostních opatření), monitorování a přezkoumávání ISMS (zajištění zpětné vazby a hodnocení řízení), údržba a zlepšování (odstraňování slabin a soustavné zlepšování).

Umožňuje chránit informace v organizaci během jejich získávání, zpracování, přenosu a skladování. Z tohoto pohledu je ISMS velmi důležitý pro většinu organizací jak ze soukromého, tak i veřejného sektoru.

ISMS představuje systematický a řízený proces trvalého zlepšování bezpečnosti informací podle mezinárodní normy ISO/IEC 27001 a ISO/IEC 27002.

Mezi přínosy při zavedení ISMS je na první pohled zřejmé, že ze zavedení ISMS plyne snížení pravděpodobnosti dopadu bezpečnostních incidentů. Přínosem je zajištění kompatibility v oblasti bezpečnosti s ostatními organizacemi, ujištění partnerů a zákazníků o adekvátní ochraně informací, která je z pohledu cloud computingu velmi významná. Dále je možnost získání mezinárodně uznávaného certifikátu.

Obrázek č. 2.8 zobrazuje model PDCA, neboli model Plánuj – Dělej – Kontroluj – Jednej, v souvislosti s hlavními čtyřmi etapami životní cyklu ISMS.



Obr. 2.8 PDCA Model pro řízení bezpečnosti informací (zdroj: www.cybersecurity.cz)[5]

2.11.1 Ustanovení ISMS

Ustanovení ISMS je první etapou, při které jsou upřesněny formy řešení bezpečnosti informací. Tato etapa se zaobírá definicí rozsahu ISMS a odsouhlasením Prohlášení o politice ISMS. Prohlášení o politice se zabývá provedením analýzy rizik a výběrem vhodných bezpečnostních opatření pro snížení vlivu existujících rizik.

Dle Nováka a Požára lze ustanovení ISMS rozdělit na skupiny:

- definice rozsahu, hranic a vazeb ISMS,
- definice a odsouhlasení „Prohlášení o politice ISMS“,
- analýza a zvládání rizik,
  - definice přístupu organizace k hodnocení rizik,
  - identifikace rizika včetně určení aktiv a vlastníků,
  - analýza a vyhodnocení rizik,
  - identifikace a ohodnocení variant pro zvládání rizik,
  - výběr cílů, opatření a jednotlivých opatření pro zvládání rizik,
  - souhlas vedení organizace s navrhovanými zbytkovými riziky,
- příprava Prohlášení o aplikovatelnosti.

[5]http://www.cybersecurity.cz/data/srib.pdf

Definice rozsahu, hranic a vazeb ISMS upřesňuje charakteristické činnosti a cíle organizace, organizační strukturu, umístění lokalit, používané technologie. Na základě definování těchto pojmů se v organizaci stanoví rozsah ISMS.

Druhým krokem je definice prohlášení o politice ISMS, která vzniká na základě specifických potřeb dané organizace. Z praktického hlediska je důležité, aby politika ISMS:

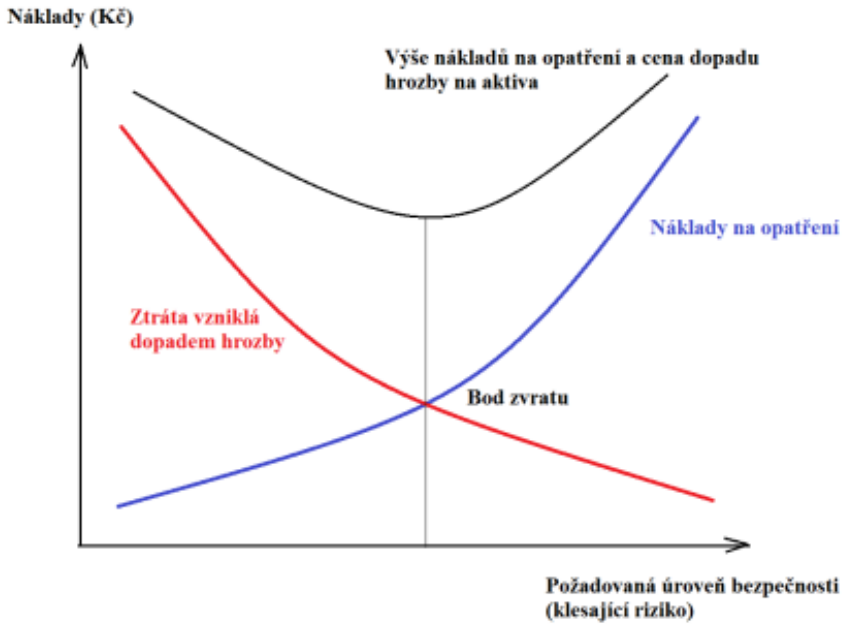
- upřesnila cíle ISMS a definovala základní směr a rámec pro řízení bezpečnosti informací,
- zohlednila cíle a požadavky organizace a související zákonné, regulativní a smluvní požadavky,
- vytvořila potřebné vazby pro vybudování a údržbu ISMS v organizaci,
- stanovila kritéria, podle kterých budou popisována a hodnocena rizika,
- byla schválena vedením organizace.

(Doucek a kolektiv, 2011, str. 88)

Analýza bezpečnostních rizik a řízení bezpečnostních rizik představuje základní nástroj k ochraně investic. Vlastní provedení procesu analýzy rizik je možné rozdělit podle podrobnosti a hloubky přístupů k jejímu řešení:

- nedělat nic,
- neformální přístup – analýza rizik se provádí živelně bez dokumentace a přesných postupů,
- základní přístup – postupy jsou rámcově zdokumentovány a organizace má celkovou koncepci a vizi v řešení bezpečnosti informací,
- detailní přístup – všechna rizika jsou analyzována podrobně podle předem definované a dodržované metodiky,
- kombinovaný přístup – některé rizika jsou analyzována podrobně, některá jsou případně při analýze i záměrně opomenuta.

Obrázek č. 2.9 znázorňuje nákladový model pro realizaci bezpečnostních opatření. Tento model vypovídá o tom, že s růstem požadované úrovně bezpečnosti exponenciálně rostou náklady na opatření.



Obr. 2.9 Nákladový model pro realizaci bezpečnostních opatření (zdroj: Doucek a kolektiv, str. 93)

Je žádoucí, aby se systém hodnocení a řízení rizik organizace opíral o stanovená kritéria pro hodnocení a akceptaci rizik. Je nutné definovat potřebné stupnice pro vyjádření veličin potřebných pro řízení rizik. Je především důležité definovat stupnice pro stanovení:

- míry důvěrnosti aktiv,
- míry integrity aktiv,
- míry dostupnosti aktiv,
- míry dopadů a škod,
- pravděpodobnosti uplatnění hrozby,
- pravděpodobnosti selhání využívaných bezpečnostních opatření,
- stupnice pro vyjádření rizik a hladiny přijatelnosti rizika.

Pro řízení rizik je důležité identifikovat hrozby, které mohou působit na aktiva firmy a negativně ovlivnit jejich hodnotu. S ohledem na hodnotu a význam dotřených aktiv se určí výše dopadu na aktivum. Na základě obecných zkušeností se určí pravděpodobnost, se kterou se daný scénář může uplatnit. Další proměnou je míra zranitelnosti a na základě bezpečnostních opatření se určuje míra účinnosti.

Pravděpodobnost vzniku a existence rizika se dělí na pět skupin – nahodilá, nepravděpodobná, pravděpodobná, velmi pravděpodobná a trvalá. Následně se stanovuje míra rizika. Míra rizika je taktéž rozdělována do pěti skupin – bezvýznamné riziko, akceptovatelné riziko, mírné riziko, nežádoucí riziko a nepřijatelné riziko.

Bezvýznamné riziko nevyžaduje žádné další zvláštní opatření, nejedná se však o 100% bezpečnost, proto je nutno o tomto riziku vědět. Toto riziko je možno přijmout a je vhodné uvést například organizační a výchovná opatření.

Akceptovatelné riziko je riziko, které je přijatelné se souhlasem vedení. Je však nutno zvážit náklady na případné řešení nebo zlepšení. Je potřeba zavést alespoň vhodná a přiměřená opatření dle místních podmínek, většinou postačuje školení.

Mírné riziko, u tohoto rizika jsou nutné bezpečnostní opatření, která se musí realizovat podle zpracovaného plánu a podle rozhodnutí vedení firmy. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období.

Nežádoucí riziko vyžaduje rychle provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnější úroveň.

Nepřijatelné riziko je nepřípustné. Hrozí možnost úrazů, závažných nehod, nastává zde nutnost okamžitého zastavení činnosti nebo odstavení z provozu a nového vyhodnocení rizik a přijetí potřebných opatření.

(Ondrák, Sedlák a Mazálek, 2013, str. 90)

Závěrečným krokem řízení rizik řeší problém, jak navrhnout vhodné formy ochrany pro podnik. Na základě zjištěných bezpečnostních potřeb je nutné vybrat vhodná bezpečnostní opatření, která umožní zjištěná rizika vhodně eliminovat. Pro zvládání rizik se nejčastěji využívá katalog opatření definovaný normou ISO/IEC 27002.

Metodiky a návrh bezpečné infrastruktury se dělí na podskupiny, kterými jsou – analýza rizik a návrh opatření, podpůrná opatření, architektura zabezpečení sítě, referenční scénáře, technické řešení „hrozba – opatření“, implementace a testování, provozování bezpečné infrastruktury, monitorování a hodnocení bezpečné infrastruktury, přínos k bezpečnosti IT, ekonomický přínos.

Na základě výsledků řízení rizik by mělo vedení podniku odsouhlasit návrh bezpečnostních opatření, která jsou nutná pro snížení bezpečnostních rizik. Dále by se vedení podniku mělo vyjádřit, zda jsou existující zbytková rizika pro chod organizace přijatelná či nikoliv.

Prohlášení o aplikovatelnosti je povinný dokument pro podnik, který usiluje o shodě svého ISMS s normou ISO/IEC 27001. Tento dokument musí obsahovat cíle opatření a jednotlivá bezpečnostní opatření, která byla pro daný ISMS vybrána na pokrytí bezpečnostních rizik.

V praxi je toto prohlášení nejdůležitějším dokumentem, který postihuje systémové vazby ISMS. Prohlášení o aplikovatelnosti obsahuje postupy nasazení bezpečnostních opatření.

2.11.2 Zavedení ISMS

Druhá etapa se zabývá zavedením ISMS a navazuje na etapu první. Zabývá se účinností bezpečnosti informací a rozsahem bezpečnosti informací, jenž naplňuje cíle organizace, a zda jsou opatření implementována správně.

Během druhé etapy zavádění ISMS je nezbytné provést následující činnosti:

- formulovat dokument Plán zvládání rizik a započít s jeho zaváděním,
- zavést plánovaná bezpečnostní opatření a zformulovat příručku o bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací,
- definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků informatiky a zejména z oblasti řízení bezpečnosti,
- upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele,
- zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty,
- řídit zdroje, dokumenty a záznamy ISMS.

(Doucek a kolektiv, 2011, str. 104)

Plán zvládání rizik je důležitým dokumentem, který popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovení cílů a priorit těchto činností ISMS. Plán zvládání rizik popisuje i omezující faktory a potřebné zdroje. Významným prvkem je též jednoznačné určení odpovědnosti za provádění jednotlivých naplánovaných činností.

2.11.3 Monitorování a přezkoumání

Hlavním úkolem třetí etapy by mělo být zajištění zpětné vazby v návaznosti na etapu první a druhou. Tato etapa se zabývá požadavkem prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Během této činnosti ISMS je nezbytné provést následující činnosti:

- monitorovat a ověřit účinnosti prosazení bezpečnosti opatření,
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,

- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace (včetně revize zbytkových a akceptovaných rizik).

(Doucek a kolektiv, 2011, str. 117)

2.11.4 Údržba a zlepšování ISMS

Čtvrtou a zároveň poslední etapou cyklu ISMS je údržba a zlepšování ISMS. Jedná se především o to, že v této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě nedostatků.

Během zavádění etapy údržby a zlepšování ISMS je nezbytné provést následující činnosti:

- zavádět identifikované množství zlepšení ISMS především na základě přehodnocení vedením,
- provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků.

(Doucek a kolektiv, 2011, str. 119)

2.11.5 ISMS v akademickém prostředí

Akademické prostředí poskytuje svým zaměstnancům internetové připojení, stává se i poskytovatelem internetového připojení pro studenty. Je tedy důležité řádné oddělení sítí – síť pro zaměstnance, síť v počítačových učebnách, wi-fi síť. Při rozdělování sítí pak nastává problém s přístupovými právy, dodržováním IT standardů, funkčním připojením zařízení od různých výrobců, zejména tedy v případě wi-fi sítě a studentských počítačů, mobilních telefonů či chytrých zařízení.

Následně se musí dodržovat AAA, princip založen na autentizaci a autorizaci jednotlivých uživatelů. Při principu AAA je důležité sledovat aktivitu, neboli logování aktivit uživatelů, tím se samozřejmě nemíní sledování každého kroku, ale přihlášení, odhlášení, použité služby.

Adekvátní bezpečnostní politika je velmi důležitým faktorem v akademickém prostředí, je potřeba se věnovat (dočasnému) omezení přístupu k wi-fi (či jiný postih) za případné ohrožení sítě či jiného porušování pravidel nebo zneužívání sítě, znemožnění instalace dalšího software pro studenty, a tak dále. Mimo jiné jsou důležitá i opatření zabezpečení sítě.

3 Analýza stavu řízení rizik na VŠ

Pro analýzu stavu řízení rizik na vysokých školách v České republice je použitý dotazník – Průzkum stavu informační bezpečnosti na veřejných vysokých školách v České republice. Tento dotazník se skládá ze tří částí. Tyto části se nazývají: otázky k organizační bezpečnosti, otázky k síťové bezpečnosti a otázky k řízení a zvládání rizik. Diplomová práce se věnuje tématu řízení a zvládání rizik, proto byla vyhodnocena a použita tato část.

Kritériem bylo místo působení vysokých škol a univerzit, průzkum byl určen pro veřejné vysoké školy v České republice. Připojena jsou taktéž grafická vyhodnocení, ze kterých autor vyvodil příslušné závěry.

Kromě dotazníku, na který odpovídali zástupci vysokých škol a univerzit v České republice, byl vytvořen dotazník pro studenty Vysoké školy báňské – Technické univerzity Ostrava, který zjišťuje jejich postavení a názor na cloud computing, CC technologie a využití CC při studiu. Kritériem pro vyhodnocení tohoto dotazníku bylo to, aby student navštěvoval VŠB-TU Ostrava. Taktéž jsou připojena grafická vyhodnocení, ze kterých autor vyvodil příslušné závěry.

3.1 Průzkum stavu informační bezpečnosti na veřejných vysokých školách v ČR

Dotazník, na který odpovídali zástupci veřejných vysokých školy, se skládá ze čtyř částí. První část je věnována bezpečnostním incidentům. Dále pak je vyhodnocen dopad incidentu a jsou vyhodnoceny přímé finanční náklady a časové výpadky systému při incidentu. Druhá část je věnována otevřeným otázkám:

- jak rychle jste byli schopni detekovat bezpečnostní incidenty od okamžiku jejich zachycení?,
- máte zaveden systém monitorování bezpečnostních incidentů?,
- máte definovány postupy reakce na výskyt bezpečnostních incidentů?,
- má Vaše vysoká škola/univerzita vypracované a připravené plány obnovy funkčnosti informačního systému?,
- jsou tyto plány obnovy pravidelně testovány?,
- kdy naposled byla na Vaší škole provedena analýza rizik IS?,
- jakým způsobem řešíte informační bezpečnost na Vaší vysoké škole?,
- byla oblast informační bezpečnosti posouzena externím subjektem (například audit nebo bezpečnostní certifikace)?,

- v jakých intervalech se připravují interní zprávy/reporty pro oblast informační bezpečnosti na Vaší vysoké škole/univerzitě?,
- monitoruje anebo omezuje se používání Internetu pracovníků?,
- využíváte v rámci svých činností elektronický podpis?,
- jaký je vliv zákona o ochraně osobních údajů na informační bezpečnost Vaší vysoké školy?,
- jak hodnotíte úroveň informační bezpečnosti na vysokých školách v ČR (České republice) ve vztahu k západoevropským státům?.

Třetí část dotazníku se zabývá hodnocením oblasti bezpečnosti, a která z těchto oblastí je považována za největší výzvu z hlediska bezpečnosti.

Poslední část je věnována překážkám rychlejšího prosazování informační bezpečnosti na veřejných vysokých školách v České republice.

3.2 Průzkum ohledně využívání cloud computingových služeb na VŠB-TUO

Tento dotazník je vytvořen pro studenty Vysoké školy báňské – Technické univerzity Ostrava. Taktéž je rozdělen do několika částí. První část se zabývá tím, zda má respondent povědomí o tom, co pojem cloud computing znamená.

Druhá část se zabývá využíváním cloud computingových technologií na VŠB-TU Ostrava. Třetí část se zabývá portálem lms.vsb.cz. Předposlední část se zabývá řízením a zvládáním rizik, poslední část je pak věnována osobním údajům respondentů.

4 Vyhodnocení průzkumu

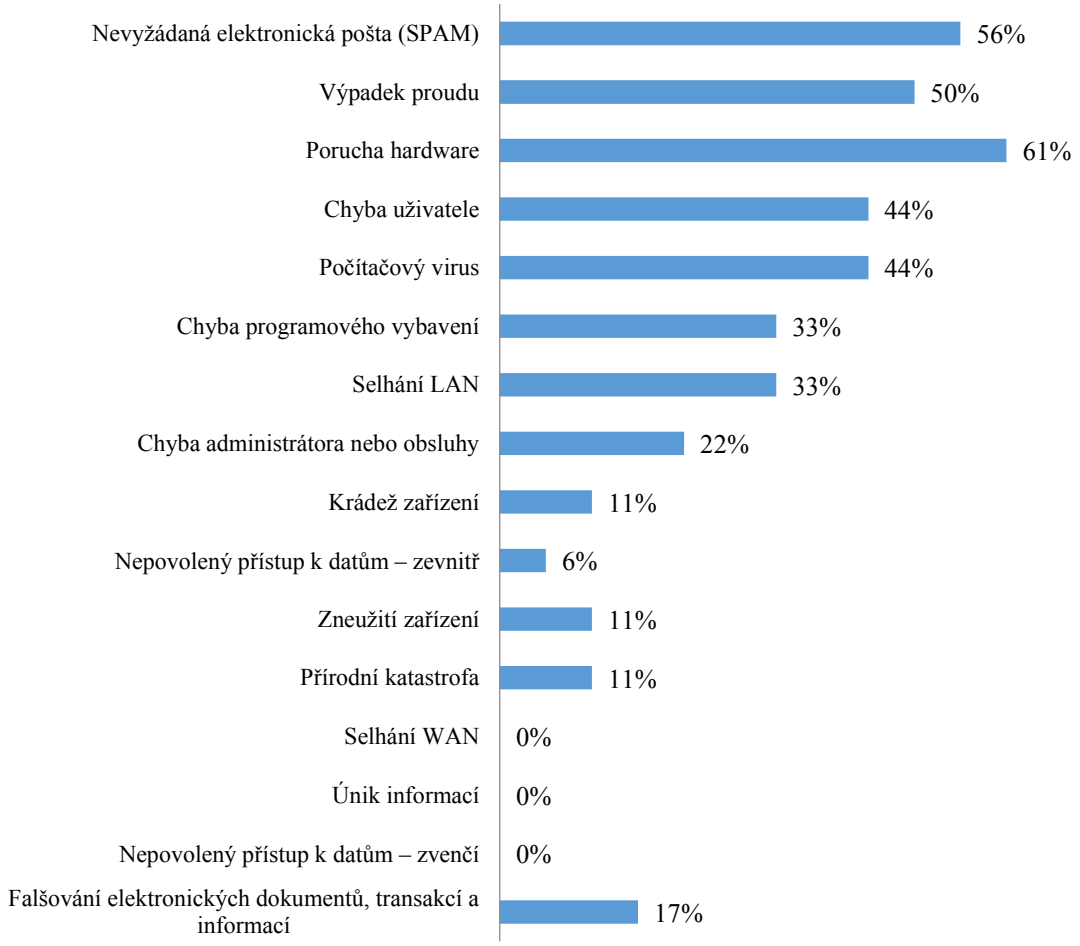
4.1 Průzkum stavu informační bezpečnosti na veřejných vysokých školách v ČR

Na dotazník odpovídali zástupci z osmnácti veřejných vysokých škol či univerzit. V části řízení a zvládání rizik respondenti neodpovídali na všechny otázky. Z toho důvodu jsou upraveny konečné počty respondentů pro každou otázku. Respondenti, kteří na otázku neopověděli, jsou vyřazeni, aby neovlivnily konečné výsledky.

Jak již bylo zmíněno, průzkum byl rozdělen do čtyř částí.

4.1.1 Bezpečnostní incidenty

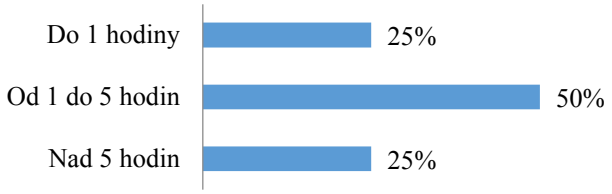
V první části průzkumu řízení a zvládání rizik respondenti vybírali bezpečnostní incidenty, které zaznamenali za poslední dva roky a k těmto incidentům připojili hodnocení dopadu, odhadované přímé finanční náklady a odhadované časové výpadky systému vysoké školy.



Graf 4.1 Bezpečnostní incidenty (zdroj: autor)

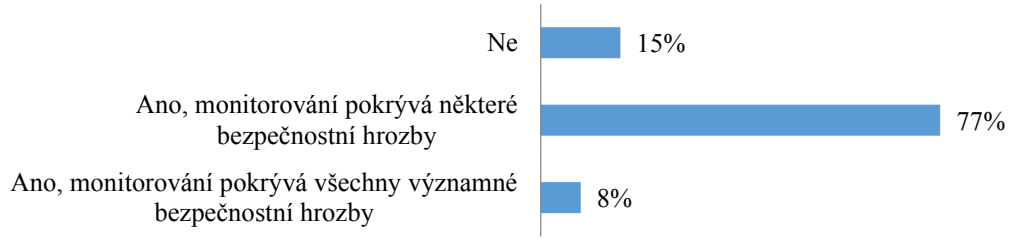
Vysoké školy i univerzity musí čelit bezpečnostním incidentům, což potvrzuje význam informační bezpečnosti a potřebu zaměření se na tuto oblast. Graf č. 4.1 znázorňuje, že nejčastěji zaznamenanými bezpečnostními incidenty jsou porucha hardware, nevyžádaná elektronická pošta či výpadek proudu. Na druhou stranu se veřejné vysoké školy nejméně nebo vůbec potýkají se selhání WAN (Wide Area Network), únikem informací a nepovoleným přístupem k datům.

Je důležité se bezpečnostním incidentům vyhýbat nebo je včas detekovat a zmírnit tak případné náklady na řešení. Graf č. 4.2 znázorňuje, že až 50% respondentů dokáže detekovat bezpečnostní incident od okamžiku jeho zachycení od jedné do pěti hodin. 25% detekuje bezpečnostní incident již do jedné hodiny a dalším 25% to trvá nad pět hodin.



Graf 4.2 Rychlost detekce bezpečnostního incidentu (zdroj: autor)

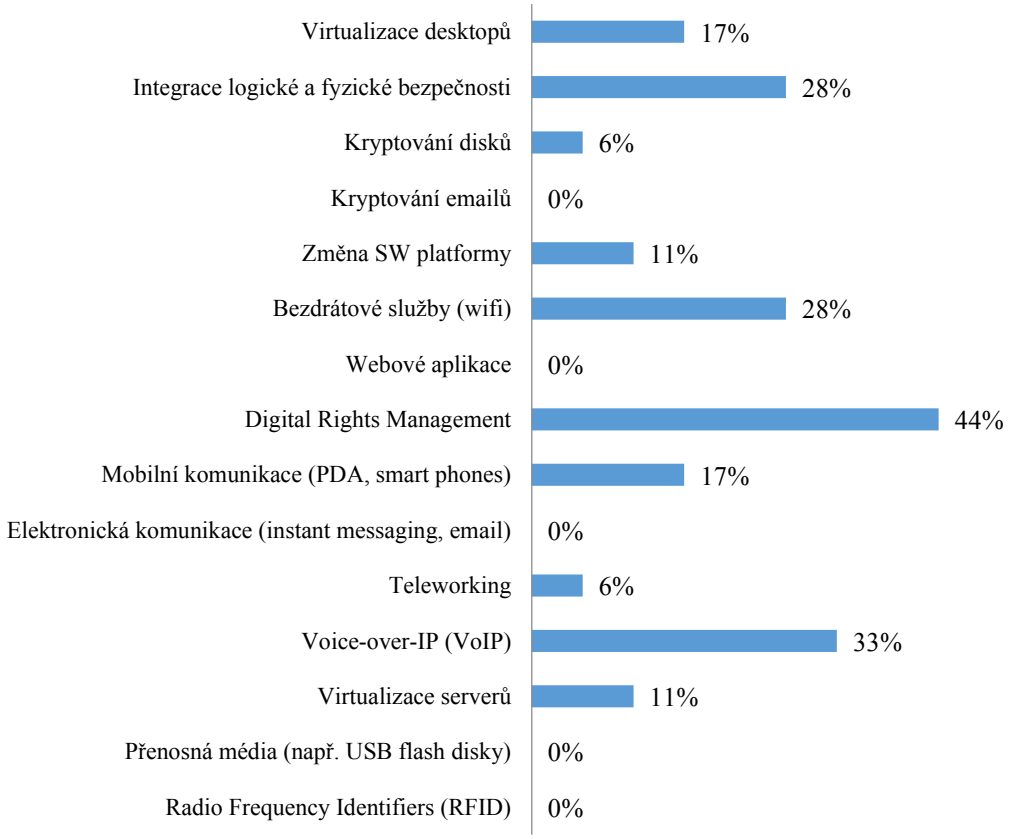
Schopnost detekce bezpečnostních incidentů prokazuje, což je uvedeno v grafu č. 4.3, že většina respondentů, dokonce až 85%, má zavedeno monitorování těchto incidentů.



Graf 4.3 Systém monitorování bezpečnostních incidentů (zdroj: autor)

4.1.2 Výzvy v rámci vysokých škol z hlediska bezpečnosti

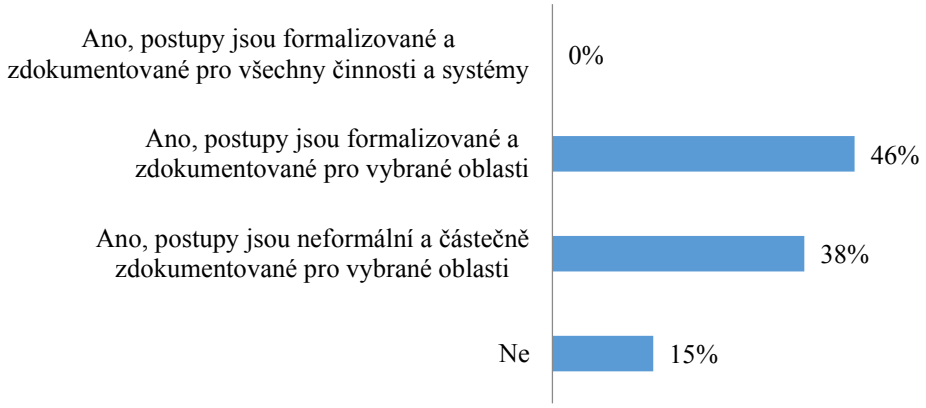
V rámci průzkumu vysoké školy odpovídaly na otázku: „Které z těchto oblastí považujete v rámci Vaší vysoké školy za největší výzvu z hlediska bezpečnosti?“. Graf č. 4.4 zobrazuje, že z hlediska bezpečnosti jsou pro většinu respondentů největšími výzvami Digital Rights Management, Voice-over-IP (VoIP) a integrace logické a fyzické bezpečnosti a následně bezdrátové služby (wifi).



Graf 4.4 Výzvy z hlediska bezpečnosti (zdroj: autor)

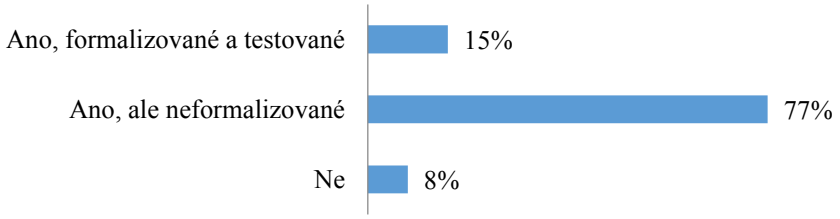
4.1.3 Otevřené otázky

Respondenti odpovídali na otázku, zda mají definovány postupy reakce na výskyt bezpečnostních incidentů. Téměř polovina uvedla, že jejich vysoká školy tyto postupy má formalizované a zdokumentované pro vybrané oblasti. Dále je zajímavé, že ani jedna vysoká veřejná škola nemá tyto postupy formalizované a zdokumentované pro všechny činnosti a systémy a dokonce jeden z respondentů odpověděl, že takto definované postupy vůbec nemají.



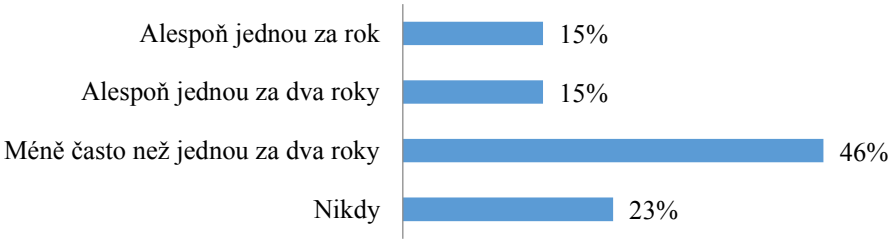
Graf 4.5 Postupy reakce na výskyt bezpečnostních incidentů (zdroj: autor)

Respondenti odpovídali na otázku týkající se plánu obnovy. Plán obnovy funkčnosti systému hraje v oblasti řízení informační bezpečnosti důležitou roli. Graf č. 4.6 zobrazuje, že téměř 95% respondentů má vypracované plány obnovy, avšak 77% nemá tyto plány formalizované.



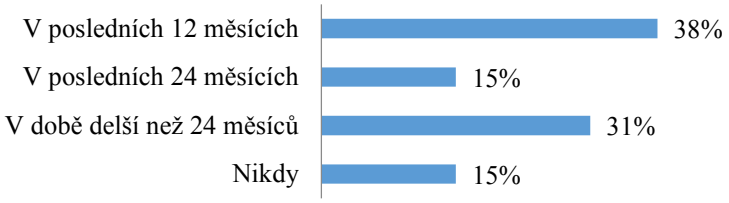
Graf 4.6 Vypracované a připravené plány obnovy funkčnosti informačního systému (zdroj: autor)

Testování umožňuje prověřit funkčnost plánu obnovy a tím i možné nedostatky. Z grafu č. 4.7 lze vyčíst velmi zajímavý údaj a tím je, že 23% respondentů nikdy netestovalo funkčnost plánu obnovy a téměř polovina testuje tento plán méně často než jednou za dva roky. Lze předpokládat, že pokud plány nikdy testovány nebyly, tak mohou být neúčinné.



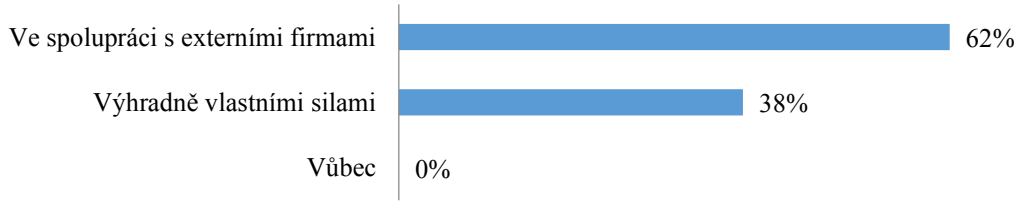
Graf 4.7 Testování plánu obnovy (zdroj: autor)

Dalším aspektem, kterým se průzkum zabývá, je analýza rizik, která představuje základ systému řízení informační bezpečnosti. Analýza rizik určuje, jaké hrozby jsou relevantní a jaký mohou mít tyto hrozby dopad. Graf č. 4.8 zobrazuje, že analýza rizik na 38% vysokých škol či univerzit proběhla v posledních 12 měsících, v době delší než je rok tuto analýzu rizik provedlo 31% a dokonce 15% respondentů analýzu rizik nikdy neprovedlo.



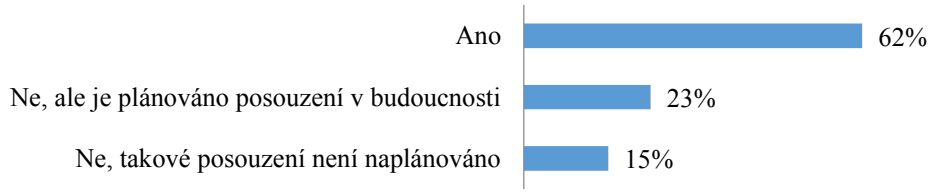
Graf 4.8 Analýza rizik IS (zdroj: autor)

Graf č. 4.9 zobrazuje výsledky, kdy 62% vysokých škol či univerzit odpovědělo na otázku: „Jakým způsobem řešíte informační bezpečnost na Vaší vysoké škole?“, ve spolupráci s externími firmami. Zbylých 38% respondentů odpovědělo, výhradně vlastními silami.



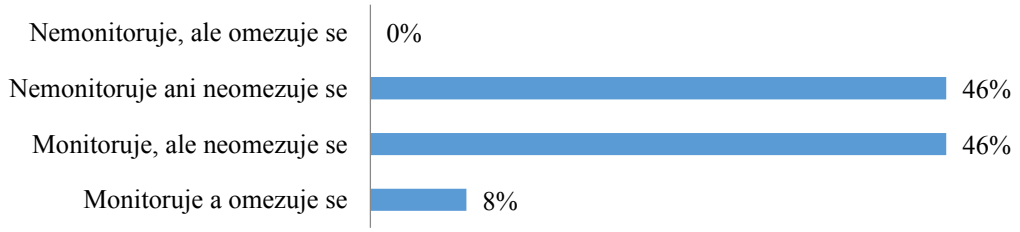
Graf 4.9 Informační bezpečnost (zdroj: autor)

Jak je možno vidět na grafu č. 4.10, 62% respondentů odpovědělo, že oblast informační bezpečnosti mají posouzenou externím subjektem, následně 23% respondentů plánuje posouzení externím subjektem. Informační bezpečnost je pro univerzitní prostředí významným faktorem.



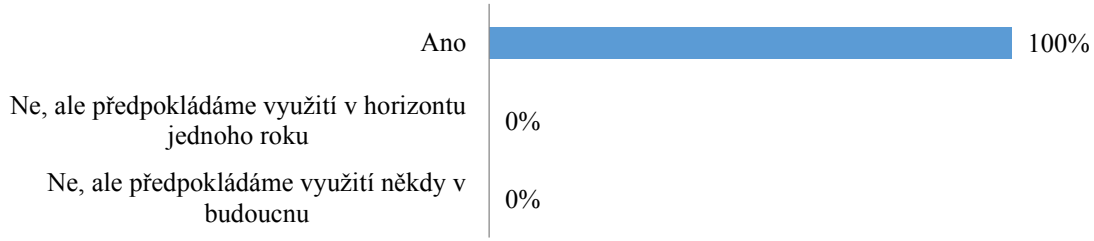
Graf 4.10 Externí subjekt (zdroj: autor)

Následující graf, tedy graf č. 4.11 se zabývá tím, zda vysoké školy či univerzity monitorují či omezují své zaměstnance. 46% respondentů uvedlo, že své zaměstnance nemonitoruje ani neomezuje. Stejný podíl odpověděl, že své zaměstnance neomezuje, avšak monitoruje. Celkově své zaměstnance omezuje 8% respondentů.



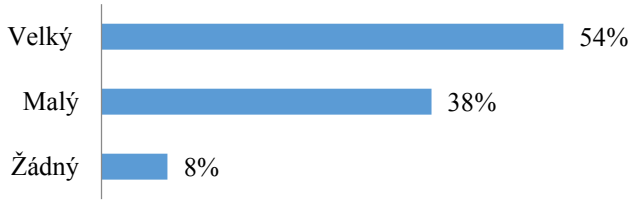
Graf 4.11 Monitorování anebo omezování zaměstnanců (zdroj: autor)

Vysoké školy či univerzity využívají elektronický podpis poměrně často, například v tomto průzkumu uvedli všichni respondenti, že elektronický podpis používají, tento výsledek je možno vidět na grafu č. 4.12.



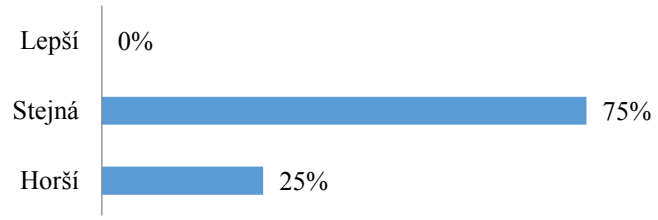
Graf 4.12 Elektronický podpis (zdroj: autor)

Následně více než polovina respondentů uvedla, že dopad zákona o ochraně osobních údajů na řešení informační bezpečnosti v rámci jejich vysoké školy je značný, výsledky jsou graficky zobrazeny na grafu č. 4.13.



Graf 4.13 Vliv zákona o ochraně osobních údajů na informační bezpečnost (zdroj: autor)

Poslední otázkou této části průzkumu byla otázka: „Jak hodnotíte úroveň informační bezpečnosti na veřejných vysokých školách v ČR ve vztahu k západoevropským státům?“. 75% respondentů uvedlo, že hodnotí úroveň informační bezpečnosti na veřejných vysokých školách v ČR ve vztahu k západoevropským státům, stejně. Dále pak žádný respondent neuvedl, že by úroveň informační bezpečnosti byla lepší ve vztahu k západoevropským státům, výsledky jsou zobrazeny na grafu č. 4.14.

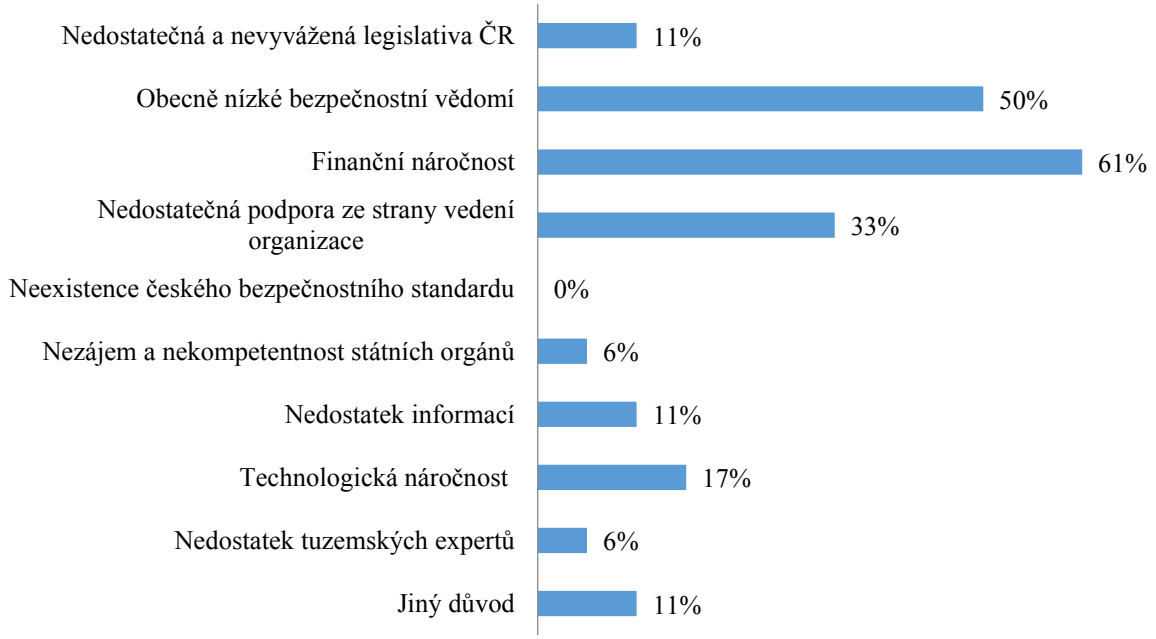


Graf 4.14 Úroveň informační bezpečnosti na vysokých školách v ČR (zdroj: autor)

4.1.4 Překážky prosazování informační bezpečnosti na VŠ

Graf č. 4.15 zobrazuje odpovědi na otázku, kdy respondenti měli vybrat tři hlavní překážky rychlejšího prosazování informační bezpečnosti na vysokých školách v ČR. Za největší překážky jsou považovány finanční náročnost, obecně nízké bezpečnostní povědomí a nedostatečná podpora ze strany vedení organizace.

Na druhou stranu překážky, jako neexistence českého bezpečnostního standardu, nezájem a nekompetentnost státních orgánů, nedostatek tuzemských expertů, nebyly vybírány často. Graf č. 4.15 zobrazuje procentuální rozdělení.



Graf 4.15 Překážky rychlejšího prosazování informační bezpečnosti (zdroj: autor)

4.2 Průzkum ohledně využívání cloud computingových služeb na VŠB-TUO

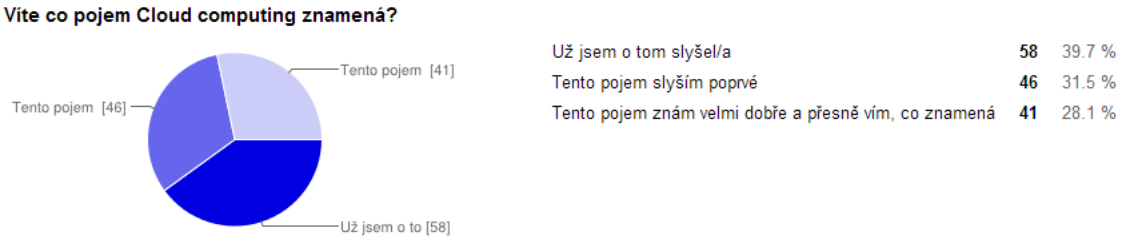
Průzkum týkající se využívání cloud computingových služeb na Vysoké škole báňské – Technické univerzitě Ostrava je zveřejněn studentům. Cílem je zjištění zda studenti mají povědomí o cloud computingu. Zda studenti vědí, co tento pojem znamená, popřípadě zda s touto technologií pracují. Následně bylo zjišťováno, zda studenti ukládají svá data do CC uložišť, zda mají o svá data strach či plně CC službám věří.

Dále pak bylo zjišťováno, zda studenti vědí či mají povědomí o finančních nákladech při zřizování a používání CC služeb. Třetí blok se zabýval portálem lms.vsb.cz a tím jak si studenti myslí, že jsou materiály zveřejňované na tomto portálu kvalitní. Poslední blok se věnoval osobním údajům studentů.

Dotazník byl vytvořen pomocí Google Apps a výstupy jsou zveřejněny graficky. Dotazník je zveřejněn v příloze.

4.2.1 Otázky týkající se využívání cloud computingu

První otázka tohoto bloku zjišťuje, zda studenti vědí, co pojem cloud computing znamená. Je zajímavé, že skoro 32% studentů odpovědělo, že tento pojem slyší poprvé, viz graf č. 4. 16. Je to zajímavý fakt, vzhledem k tomu, že cloud computing je označován za takzvaný „buzzword“. Grafický výstup je možno vidět na grafu č. 4.16.



Graf 4.16 Pojem CC (zdroj: autor)

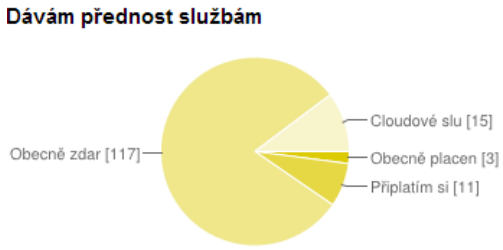
Další otázka se zabývá tím, a na grafu č. 4.17 je zobrazeno, jaké kancelářské balíčky studenti využívají. Nejčastější odpovědí bylo MS Office a následně Google Apps.

Graf 4.17 Kancelářské balíky (zdroj: autor)

Graf č. 4.18 zobrazuje odpovědi studentů na otázku, zda využívají on-line řešení pro tvorbu školních dokumentů. Zda používají sdílené dokument a nad sdíleným dokumentem zároveň pracují. Větší část respondentů odpovědělo, že ano.

Graf 4.18 On-line řešení pro tvorbu školních dokumentů (zdroj: autor)

Další otázka se zabývá tím, jak placené služby studenti využívají. Naprostá většina, 80% odpověděla, že dává přednost cloud computingovým službám, které jsou zdarma, a pouze 2% používá služby placené.



Obecně placeným	3	2.1 %
Připlatím si rád za řešení od firmy, kterou preferuji.	11	7.5 %
Obecně zdarma	117	80.1 %
Cloudové služby nepoužívám	15	10.3 %

Graf 4.19 Služby (zdroj: autor)

Graf č. 4.20 se zabývá tím, jak studenti chápou citlivá data v cloud computingovém uložišti. Přes polovinu respondentů si myslí, že data v cloud computingových uložištích jsou nedostatečně chráněná a citlivá data by poskytovatelům nikdy nesvěřila. Necelých 20% respondentů si myslí, že data jsou naprosto v bezpečí a s klidným svědomím by je poskytovatelům cloud computingových služeb svěřila.

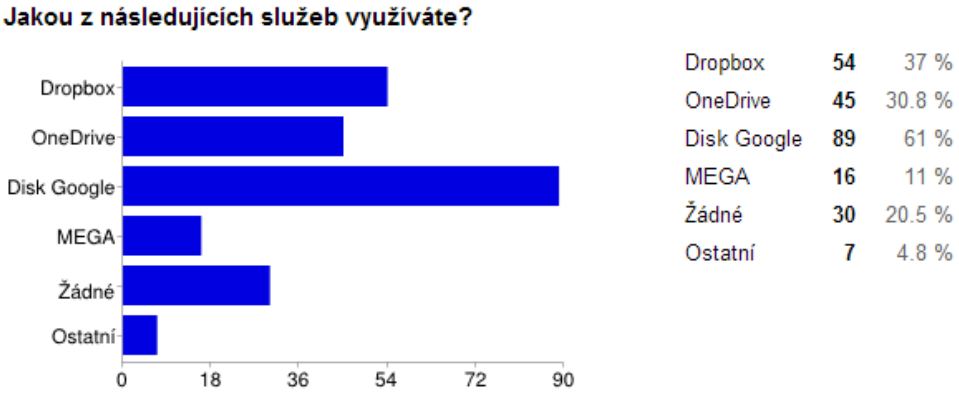
Zcela v bezpečí, klidně data svěřím poskytovatelům Cloudových technologí	26	17.8 %
Nedostatečně chráněna, citlivá data poskytovatelům nikdy nesvěřím	83	56.8 %
Nevím	37	25.3 %

Graf 4.20 Citlivá data (zdroj: autor)

Další otázka se týká toho, zda mají respondenti obavy ze zneužití svých dat v cloud computingových službách. Viz graf č. 4.21, skoro 75% respondentů má obavy ze zneužití dat, z toho 45% studentů i přes obavy cloud computingové služby využívá. 13% respondentů obavy nemá a 13% respondentů cloud computingové služby nepoužívá.

Graf 4.21 Zneužití dat (zdroj: autor)

Předposlední otázkou prvního bloku je otázka, jakou ze služeb studenti využívají. Na grafu č. 4.22 je zobrazeno, že nejčastěji používanou cloud computingovou službou je Disk Google, Dropbox a následně OneDrive.



Graf 4.22 Služby (zdroj: autor)

Poslední otázkou tohoto bloku, je otázka otevřená, která se zaměřuje na výhody a nevýhody cloud computingu z pohledu studentů. Nejčastěji je studenty jako výhoda, zmíněna dostupnost, automatické zálohování, sdílení dokumentů s více lidmi. Následně pak to, že s sebou nemusí nosit flash disk. Taktéž je několikrát zmíněno to, že cloud computing nevyužívá prostor na hard disku na počítače.

Jako nevýhody studenti zmínili bezpečnost dat. Myslí si, že data nejsou dostatečně chráněna v cloud computingové technologii. Dále pak to, že neví, kdo má přístup k jejich datům a taktéž jako nevýhodu uvedli možnou ztrátu dat.

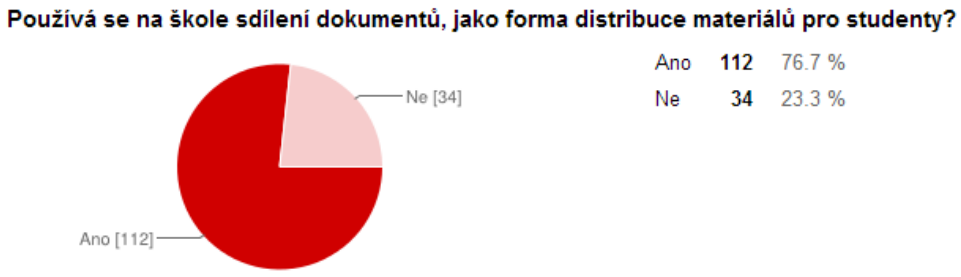
4.2.2 Využívání cloud computingových technologií na VŠB-TUO

Druhá část dotazníkového šetření se zabývá tím, zda mají studenti povědomí o tom, zda používají cloud computingové služby ve škole nebo při studiu. Následně zda mají povědomí o finanční stránce zřízení cloud computingových služeb pro vysokou školu.

První otázka se zabývá tím, zda studenti používají ve škole nějaké on-line uložiště dat. Zda si sdílí výukové materiály přes uložiště, například ulozto.cz, edisk.cz či podobné. Graf č. 4.23 zobrazuje, že 74% studentů takto nějaké datové uložiště využívá.

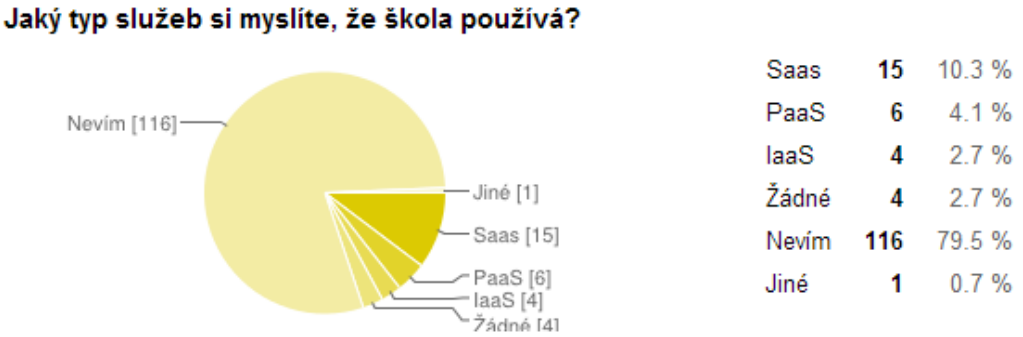
Graf 4.23 On-line uložiště (zdroj: autor)

Graf č. 4.24 se zabývá tím, jestli se používá na škole sdílení dokumentů jako forma distribuce materiálů pro studenty. 77% studentů uvedlo, že takto sdílené dokumenty přes datové uložiště dostává.



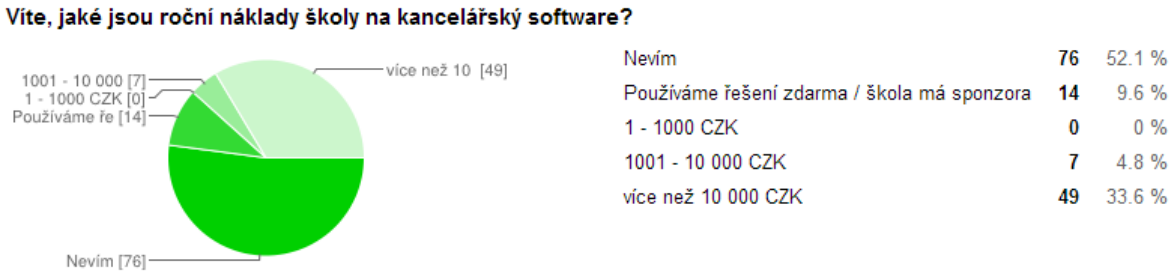
Graf 4.24 Distribuce studijních materiálů (zdroj: autor)

Další otázkou, na kterou odpovídali studenti, byla otázka ohledně typu služby cloud computingu, který je na VŠB-TUO používán, výsledky jsou zobrazeny v grafu č. 4.25. VŠB-TUO zatím žádné cloud computingové služby nepoužívá, jen 3% respondentů odpověděla správně.



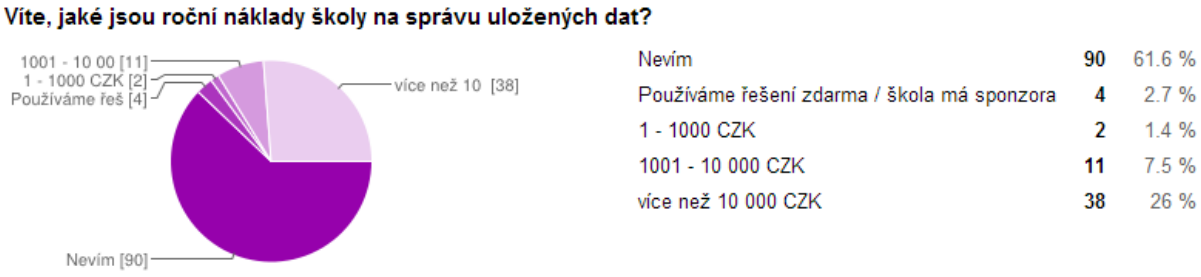
Graf 4.25 Typ služby (zdroj: autor)

Následná dvojice otázek zjišťovala, zda studenti mají povědomí o finanční stránce a možných ročních nákladech na kancelářský software a ročních nákladech VŠB-TUO na správu uložených dat. Graf č. 4.26 zobrazuje výsledky, kdy 34% respondentů uvedlo, že roční náklady jsou více než 10 000Kč na kancelářský software, popřípadě údržbu softwaru.



Graf 4.26 Náklady na kancelářský software (zdroj: autor)

Graf č. 4.27 zobrazuje výsledky, na otázku týkající se ročních nákladů na správu uložených dat, kdy 26% respondentů uvedlo, že roční náklady jsou větší než 10 000 Kč.



Graf 4.27 Finanční náklady na správu uložených dat (zdroj: autor)

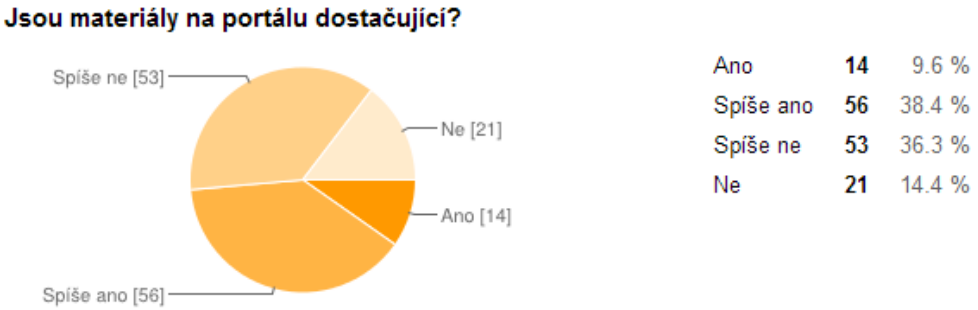
4.2.3 Portál lms.vsb.cz

Třetí část byla věnována portálu lms.vsb.cz, který studenti využívají jako učební pomůcku. Tato část zde byla zařazena, jelikož technologie a možnosti cloud computingu by portál lms.vsb.cz mohly v budoucnu nahradit. Z tohoto důvodu byla zkoumána kvalita a spokojenost studentů s výukovým portálem.

Graf č. 4.28 zobrazuje využití portálu studenty. Zda používají portál jako učební pomůcku. Více jak polovina respondentů odpověděla kladně. Dále pak 20% responedntů uvedlo spíše ano. Z toho se dá usoudit, že portál lms.vsb.cz je studenty využíván.

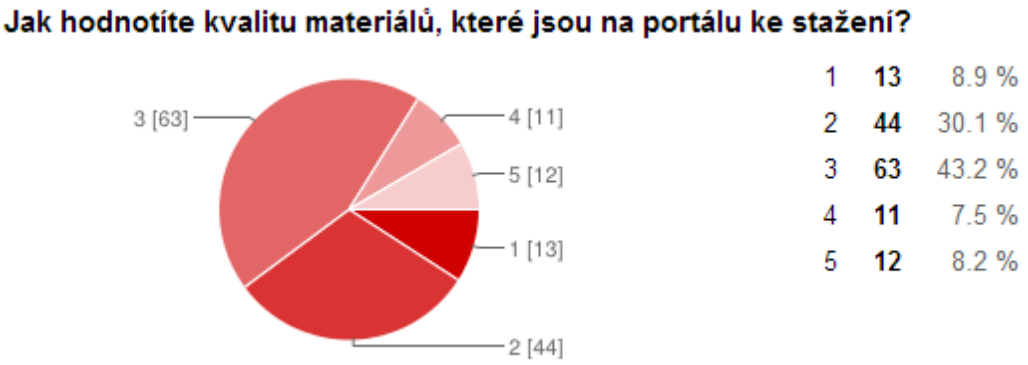
Graf 4.28 Portál jako učební pomůcka (zdroj: autor)

Další otázka zkoumá, jak studenti hodnotí kvalitu poskytovaných materiálů. Graf č. 4.29 zobrazuje, že 48% respondentů odpovědlo, že materiály jsou dostačující. Bohužel však více než 50% respondentů uvedlo, že materiály dostačující nejsou.



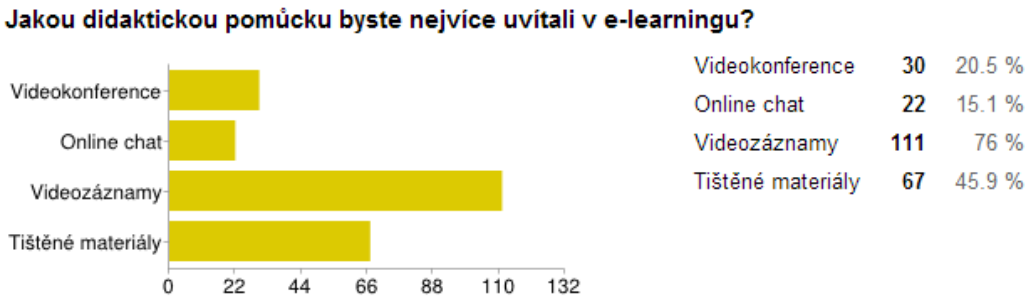
Graf 4.29 Materiály na portálu (zdroj: autor)

Následující otázka se zavývá hodnocením kvality materiálů (1 – nejlepší, 5 – nejhorší). Z grafu č. 4.30 lze vyčíst, že nejčastější známkou v hodnocení bylo číslo 3, následně číslo 2.



Graf 4.30 Kvalita materiálů (zdroj: autor)

Poslední otázkou třetího bloku zaměřujícího se na portál lms.vsb.cz je otázka týkající se další pomůcky, kterou by studenti nejvíce uvítali. 76% studentů odpovědělo videozáznam a 46% studentů by uvítalo více tištěných materiálů.

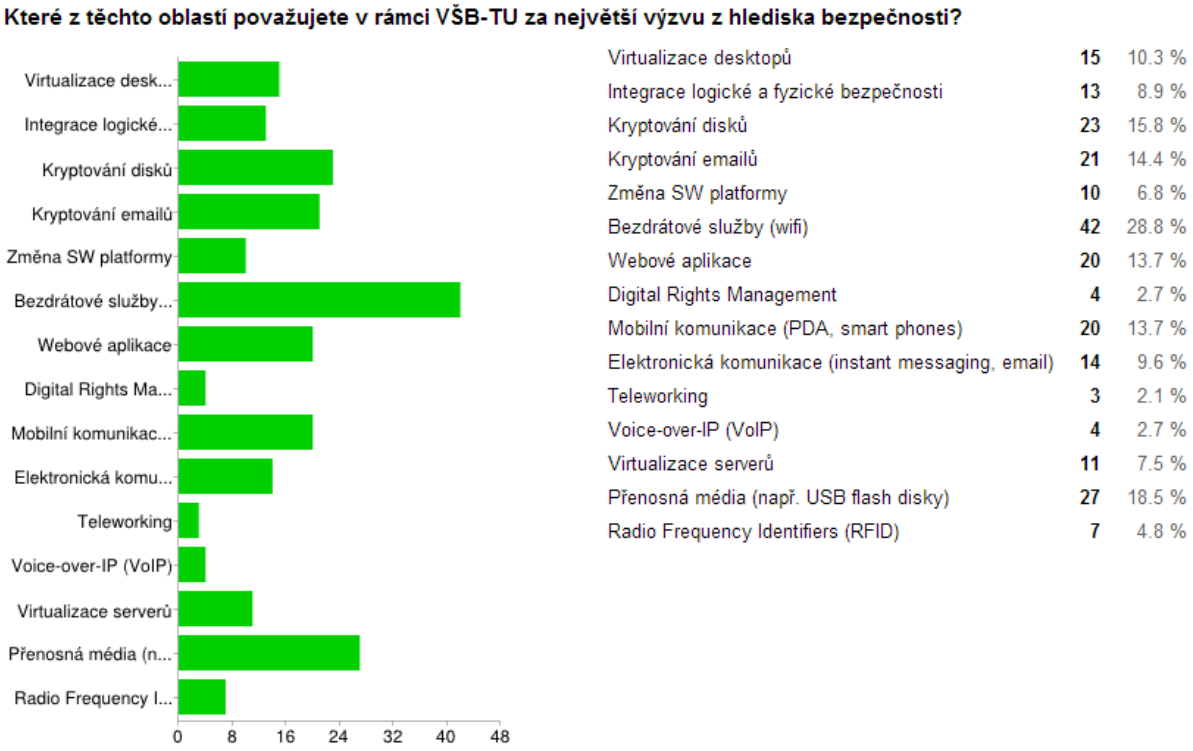


Graf 4.31 Pomůcka v e-learningu (zdroj: autor)

4.2.4 Řízení a zvládání rizik

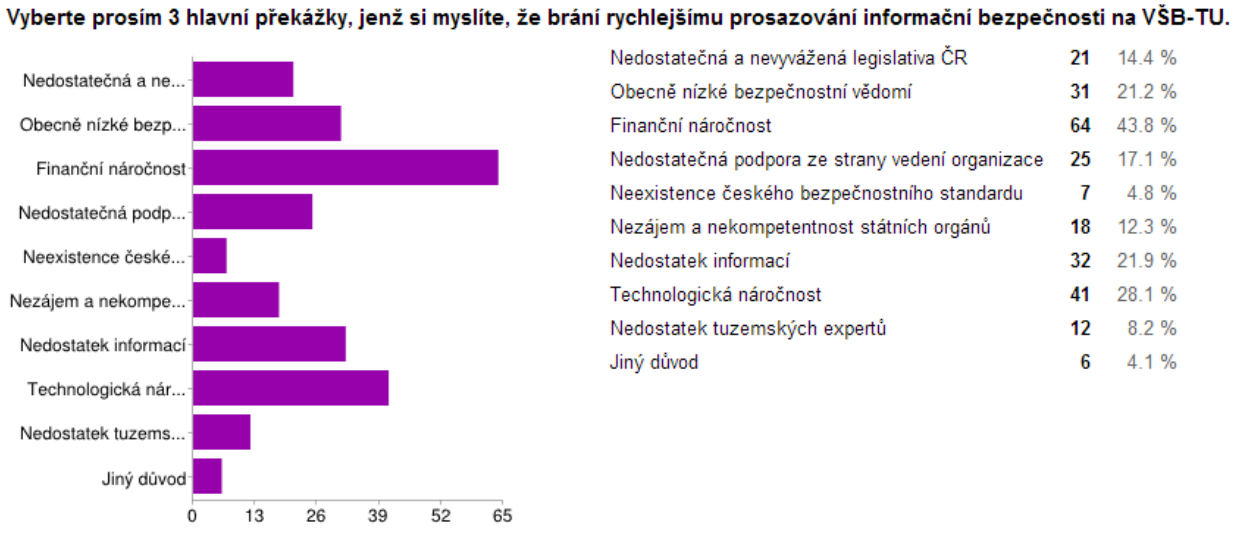
Předposlední část se zabývá problematikou řízení a zvládání rizik z pohledu studentů a jaké výzvy považují za největší z hlediska bezpečnosti. Jaké překážky si myslí, že brání rychlejšímu prosazování informační bezpečnosti na VŠB-TU Ostrava.

Graf č. 4.32 zobrazuje možné výzvy z hlediska bezpečnosti. Nejčastějšími odpověďmi studentů jsou bezdrátové služby (wifi), přenosná média (například USB flash disky) a kryptování disků. Následně pak Digital Rights Management, Teleworking a Voice-over-IP (VoIP) byly zvoleny studenty, jako nejmenší výzvy z hlediska bezpečnosti.



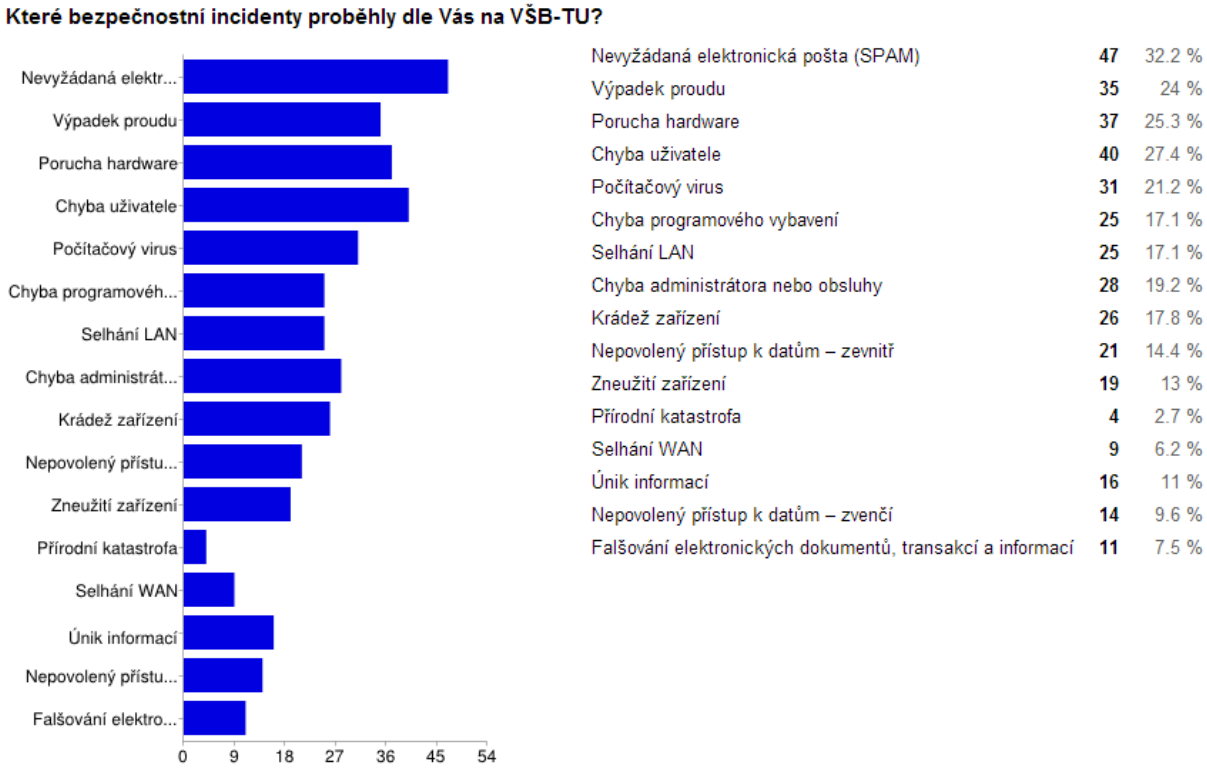
Graf 4.32 Výzvy z hlediska bezpečnosti (zdroj: autor)

Druhá otázka čtvrtého bloku se zabývá překážkami, které brání rychlejšímu prosazování informační bezpečnosti na VŠB-TU Ostrava. Studenti byli omezeni výběrem maximálně tří odpovědí a nejčastěji zvolenými odpověďmi jsou finanční náročnost, technologická náročnost a nedostatek informací.



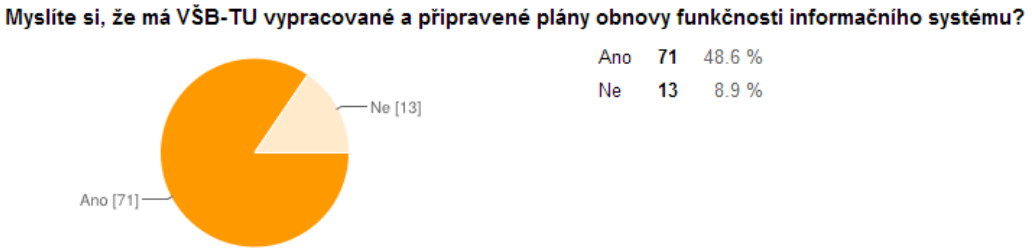
Graf 4.33 Překážky rychlejšího prosazování bezpečnosti (zdroj: autor)

Graf č. 4.34 zobrazuje odpovědi na otázku, která se zabývá bezpečnostními incidenty, které dle studentů proběhly na VŠB-TU Ostrava. Nejčastějšími odpověďmi jsou nevyžádá elektronická pošta, chyba uživatele, porucha hardware a výpadek proudu.



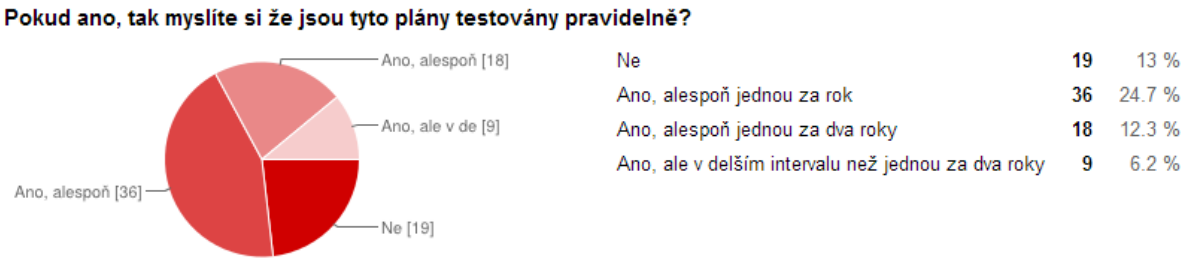
Graf 4.34 Bezpečnostní incidenty (zdroj: autor)

Další otázkou, na kterou respondenti odpovídali, byla otázka týkající se plánu obnovy a tím, zda VŠB-TU Ostrava má takovýto plán obnovy funkčnosti informačního systému vypracován a připraven. Graf č. 4.35 zobrazuje, že drtivá většina respondentů odpověděla pozitivně.



Graf 4.35 Plán obnovy a funkčnosti IS (zdroj: autor)

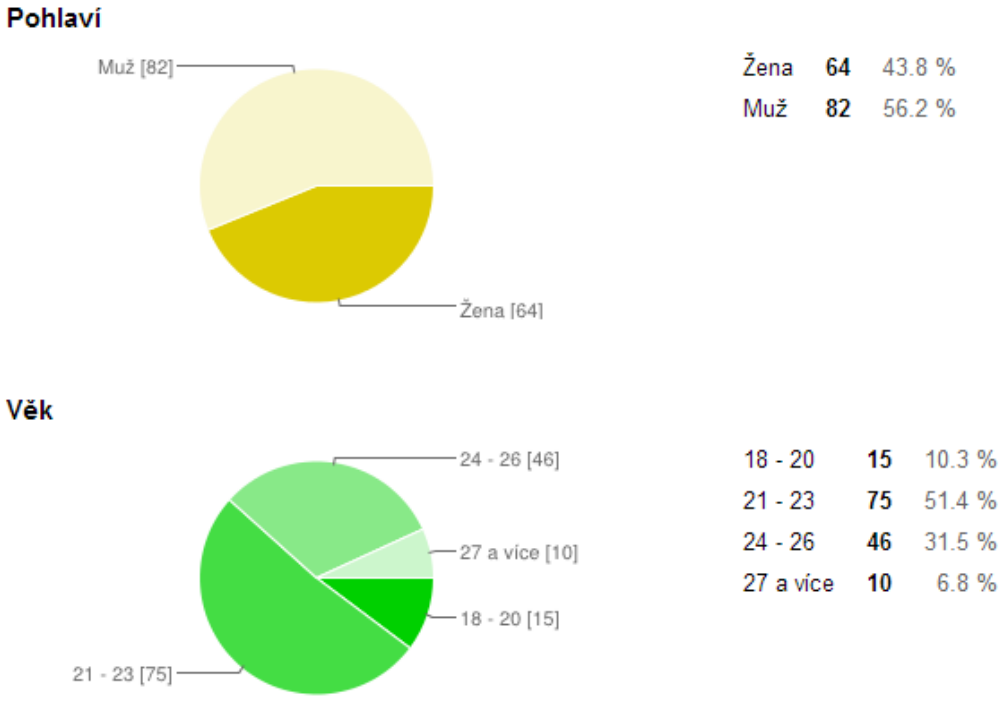
Poslední otázka, navazující na otázku předchozí, se zabývá tím, zda si respondenti myslí, že tyto plány jsou pravidelně testovány. Dle grafu č. 4.36 pozitivně odpověděla většina respondentů. Nejčastější odpovědí pak byla, že jsou tyto plány testovány alespoň jednou za rok.



Graf 4.36 Testování plánů obnovy (zdroj: autor)

4.2.5 Osobní údaje respondentů

Poslední části dotazníkového šetření byla část, kde byly zjišťovány osobní údaje. Graf č. 4.37 zobrazuje, že častěji na dotazník odpovídali muži a věk respondentů byl nejčastěji v intervalu od 21 do 23 let.



Graf 4.37 Pohlaví a věk respondentů (zdroj: autor)

Poslední otázka zjišťovala, ze které fakulty VŠB-TU Ostrava respondenti odpovídali. Nejčastěji odpovídali z Ekonomické fakulty následně z Fakulty elektrotechniky a informatiky. Nejméně respondentů je z Hornicko-geologické fakulty a Fakulty metalurgie a materiálového inženýrství. Graf č. 4.38 zobrazuje rozložení respondentů dle fakult.

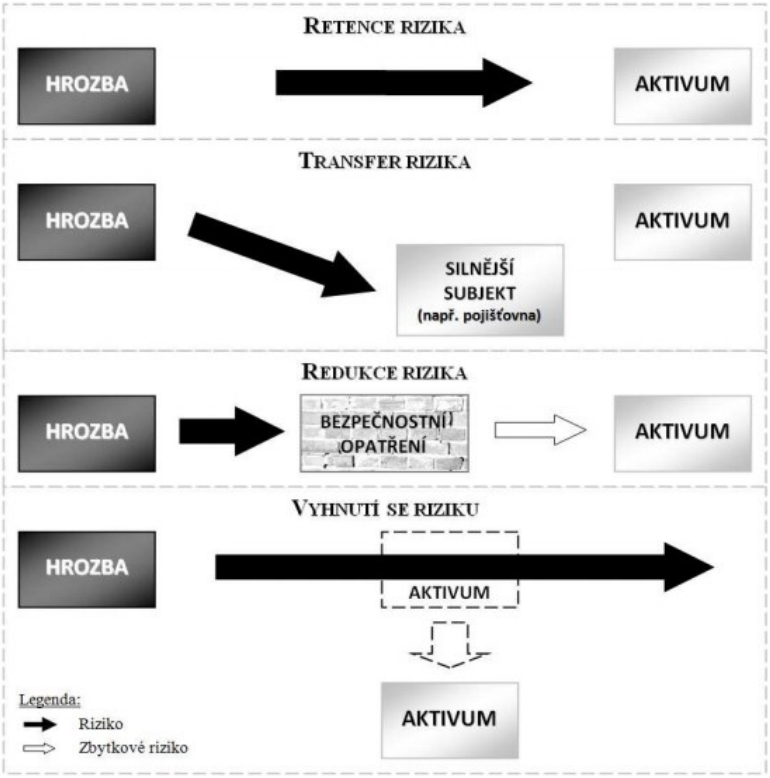
Graf 4.38 Fakulty (zdroj: autor)

5 Návrh doporučení zvládání rizik na VŠ

Z průzkumu, na který odpovídali zástupci veřejných vysokých škol, vyplynulo, že jako největší hrozby považují poruchu hardware, nevyžádanou elektronickou poštu (SPAM) a výpadek proudu. Studenti pak nejčastěji odpovídali, že největší hrozby pro bezpečnost vysoké školy považují nevyžádanou elektronickou poštu, chybu uživatele a porucha hardware. Pro tyto zmíněné rizika jsou navrhnuta doporučení pro zvládání. Kromě výše zmíněných rizik jsou vybrána i rizika jako je chyba programového vybavení a selhání LAN a pro tyto rizika jsou taktéž navrhnuta možná doporučení opatření.

5.1 Zvládání rizik

Zvládání rizik je proces, který eliminuje rizika, která byla vybrána studenty a veřejnými vysokými školami. Tento proces se snaží rizika elimininovat či jim úplně zabránit. Možnostmi jak se vyhnout rizikům jsou retence rizika, transfer rizika, redukce rizika a vyhnutí se riziku, jak je možno vidět na obrázku č. 5.1. Při procesu výběru opatření je nutno přihlédnout na faktory, kterými jsou právní požadavky, finanční, časová a technická náročnost. Dále pak můžou být zmíněny kulturní a etické kodexy.



Obr. 5.1 Zvládání rizik (zdroj: Řehák)

Zvládání rizik zahrnuje samotné zvládání rizik a následné rozhodnutí o zbytkové úrovni rizika, zda je přijatelná nebo ne.

5.1.1 Retence rizika

Retence rizika je legitimní a pravděpodobně nejběžnější metodou zvládání rizik. Spočívá v tom, že organizace čelí téměř neomezenému počtu rizik, ovšem ve většině případů proti nim nic nedělá. Retence rizik může být vědomá či nevědomá. K vědomé retenci rizika dochází tehdy, je-li riziko rozpoznáno a nedojde k aplikaci některé z jiných možností zvládání rizika (např. formou jeho transferu nebo redukce). Pokud není riziko rozpoznáno, je nevědomě zadrženo. V těchto případech organizace nikterak neřeší důsledky možných ztrát, jelikož si jejich vznik ani neuvědomuje. Retence rizika může být rovněž dobrovolná nebo nedobrovolná. Dobrovolná retence rizika je charakterizována rozpoznáním existence rizika a tichým souhlasem s převzetím v něm obsažené ztráty. Rozhodnutí o dobrovolné retenci rizika je přijímáno proto, že neexistují žádné lepší varianty. Nedobrovolná retence rizik existuje tehdy, jsou-li rizika nevědomě zadržena, anebo pokud riziko nemůže být transferováno či redukováno, případně pokud se mu nelze vyhnout. (Smejkal a Rais, 2013, str. 172)

5.1.2 Redukce rizika

Při redukci rizika musí být vybrána opatření, která jsou účinná, přijatelná, efektivní a včasná. Redukci rizika je možno realizovat dvěma přístupy, první přístup se zabývá přesunem rizika a druhý přístup se specializuje na diverzifikaci a pojištění.

5.1.3 Transfer rizika

Transfer rizika má defenzivní přístup k riziku, tento přístup se nesnaží riziko eliminovat, ale přesune riziko na jiné podnikatelské subjekty. Mezi nejčastější způsoby přesunu rizika patří uzavírání dlouhodobých kupních smluv za předem stanovené ceny (eliminace možného inflačního rizika), termínované obchody, leasing (přesun finančního rizika), odkup pohledávek a další. (Smejkal a Rais, 2013, str. 174)

5.1.4 Vyhnutí se riziku

Vyhnutí se riziku je poslední legitimní možností zvládání rizik, jež spočívá v neuskutečnění dané aktivity. Jedná se však o přístup spíše negativní, než pozitivní, který je pro řešení mnoha rizik zcela nevyhovující.

5.2 Nevyžádaná elektronická pošta (SPAM)

Nevyžádaná elektronická byla zvolena veřejnými vysokými školami i studenty, jako jednou z hrozeb.

Nevyžádaná pošta je dnes běžnou součástí elektronické komunikace. Její dopad má vliv na dostupnost klientů, kteří mají e-mailové schránky. Dále je ohrožena firemní komunikace, která probíhá zejména skrz elektronickou poštu, a to jak vnitřní, tak vnější. Ve vnitřní komunikaci je kritický dopad na příjem automaticky generovaných zpráv, které upozorňují na neobvyklé záznamy v logovacích souborech. Vzhledem k rozšířenosti a dopadu je riziko vysoké.

Jelikož dopad rizika je vysoký, proto je doporučeno se bránit proti nevyžádané elektronické poště. Obranou může být stížnost providerovi, filtrování a blokování spamu, skrývání adres a další. Stížnost providerovi však obvykle nemá žádný efekt, avšak existují specializované programy a služby, které umožňují proces identifikace správných adres a hlášení spamu za uživatele.

Ze statistiky týdeníku časopisu IT Systém vyplynulo, že podíl spamu v e-mailové komunikaci v loňském roce dosáhl 66,8%[6].

Filtrování a blokování spamu je nejpoužívanější metoda obrany. Jedním ze způsobů je blokování na základě černé listiny odesílatelů nebo podle obsahu zprávy.

Správce může poštovní server nakonfigurovat tak, aby při příchodu každého dopisu vyslal dotaz, zda stroj, od kterého zprávu přijímá, nemá záznam v některé černé listině. V kladném případě poštu z daného místa odmítnout. Blokování podle obsahu zprávy se provádí pomocí programů, tyto programy se pokouší odhalit spam, pomocí výskytu určitých slov či frází v textu. Spolehlivost takových programů nemusí být vždy uspokojivá, ale u těch nejlepších se spolehlivost zjištění spamu pohybuje kolem 60 – 70%. Mezi filtrovací programy například patří Spam Eater Pro, jenž je dostupný ve verzi freeware a shareware, dále pak Brightmail, který používají i nejvýznamnější američtí internetoví připojovatelé.

Skrývání adres je často používanou preventivní metodou obrany proti spamům a mezi obvyklá doporučení jsou uváděna například neposkytování své elektronické adresy na potkání (například uvádění e-mailové adresy na formulářích), neuvádění adresy v textu

[6] http://www.systemonline.cz/zpravy/podil-spamu-v-e-mailove-komunikaci-dosahl-loni-66-8-z.htm

příspěvků, dále pak maskování e-mailové adresy (například při uvádění e-mailové adresy nahrazovat znak @), dalším doporučením je neklikat u předchozího spamu na odkazy „removeme“ nebo „deletefrom list“.

Ochrana proti nevyžádané poště je důležitá, je proto žádoucí se proti spamové poště bránit. Existují i antispamové technologie jako například Sender Policy Framework, Domain Keys, DNSBL, SURBL, Greylisting či Bayesiánské filtry. Princip Bayesiánského filtru je založen na tom, že provádí statistickou analýzu zpráv a podle pravděpodobnosti určuje, zda je zpráva spam. Greylisting je ochrana SMTP serveru, která využívá jeho vlastnosti. Dále jsou využívány různé antispamové doplňky, které se využívají u e-mailové schránky. Například Gmail od společnosti Google má možnost pod nabídkou Rozšířené nastavení konfigurovat seznam povolených adres, příchozí bránu, nastavení pravidel pro antispamovou ochranu či dokonce blokování odesílatele.

5.3 Porucha hardware

Z průzkumu pro veřejné vysoké školy vyplynulo, že porucha hardwaru je zvolena jako největší riziko. Riziko jako porucha hardwaru či poškození zálohovacího média je pro vysokoškolské prostředí nereálné. Tato hrozba má vliv na zálohy dat, osobní údaje studentů, profesorů a popřípadě další data uložená na médiích.

Je důležité zavést efektivní a bezpečné zálohování dat.

Základní myšlenkou cloud computingu je ta, že všechny aplikace pracují na internetu a uživatel si nemusí obstarávat žádný softwaru a hardware, dále pak cloud computing snižuje nebezpečí ztráty či odcizení dat používáním centralizovaného uložení dat a používáním tenkých klientů. Riziko poruchy hardwaru na sebe přebírá poskytovatel cloud computingu, který je zodpovědný poskytovat službu, technicky a organizačně zajistit bezpečnost poskytované služby. V souladu se zákonem na ochranu osobních údajů osob, následně pak informovat o specifikovaném riziku porušení bezpečnosti sítě.

Mezi doporučená ustanovení patří ta že, poskytovatel bude provádět pravidelné bezpečnostní audity IT technologií, bude poskytovat platnou certifikaci. Dále pak zákazník musí mít on-line přístup k systémovým informacím, ze kterých je možné zjistit aktuální lokaci jeho dat. Zákazník by měl být informován o případných výpadcích služby a technických záležitostech výpadku. (Donát, 2011)

5.4 Chyba uživatele

Cloud computing se snaží být pro uživatele co nejpřívětivější a snadno pochopitelný. I přesto existují uživatelé, kteří si nešťastnou náhodou smaží data, která potřebují. Cloud computing nabízí možnost ukládání historie dat a v případě jakékoliv nehody musí být poskytovatel provést kompletní obnovu dat. Kompletní obnova dat je eliminována určitým časovým obdobím, proto je důležité vědět dobu trvání případné obnovy dat. Dále pak cloud computing nabízí synchronizaci dat rovnou do uživatelova počítače.

Avšak nejlepším doporučením je číst manuály a i přes přívětivé a známé prostředí vědět, na co je kliknuto a znát případný následek.

Mezi opatření pro uživatele patří mimo jiné nevyzrazování hesel či zneužívání firemního e-mailu. Každý uživatel musí být jednoznačně určen uživatelským jménem, velké množství neúspěšných pokusů o přihlášení by mělo vést k dočasné blokaci atd.

5.5 Selhání LAN

Dostupnost sítě je přenesena na poskytovatele internetového připojení, jelikož cloud computingové služby jsou on-line. Připojení k síti je důležité pro využívání cloud computingu. Avšak ke snížení rizika výpadku LAN sítě by se měly monitorovat aktivní prvky sítě a taktéž je vhodné kontrolovat dostupnost a zátěž zařízení používaných v síti.

5.6 Chyba programového vybavení

Ke snížení rizik chyby programového vybavení přispívá vedení záznamů o instalaci a záznamů o aktualizování programu. Díky takovému to opatření bývá možnost odhalení chyby větší a je možno vrátit systém do původního stavu. Před významnými aktualizacemi by měla být provedena záloha. Avšak cloud computing tuto chybu přenáší na poskytovatele, který poskytuje programové vybavení a je tedy jeho povinností se o toto vybavení starat a aktualizovat ho.

6 Závěr

Cílem diplomové práce bylo navrhnout doporučení pro řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na veřejných vysokých školách. Práce se zaměřuje na problematiku řízení a zvládání rizik bezpečnostních hrozeb v cloud computingovém prostředí.

Problematice cloud computingovým technologiím je věnována část druhé kapitoly, je přiblížen pojem cloud computing pomocí několika definic. Jsou uvedeny modely nasazení a distribuce. Kromě cloud computingového prostředí je zmíněno i prostředí mobilní. Druhá kapitola je věnována problematice řízení rizik bezpečnosti informací. Zde jsou popsány pojmy týkající se informační bezpečnosti, požadavky ochrany pro informační bezpečnost, dále je kapitola věnována legislativě a normám pro práci s utajovanými informacemi. Práce je zaměřená na bezpečnostní hrozby v cloud computingu a na požadavky ochrany informační bezpečnosti v CC.

Třetí kapitola se zabývala přiblížením dotazníků, které byly použity pro průzkumy řízení a zvládání rizik. Byly použity dva dotazníky, z nichž první byl zaměřen na veřejné vysoké školy a univerzity v České republice. Druhy dotazník byl zaměřen na studenty VŠB-TUO. Dotazníky byly vyhodnoceny a popsány jak slovně, tak graficky. Bylo zjištěno, že studenti vědí o cloud computingu, popřípadě s ním už pracují. Velká skupina studentů využívá nejčastěji cloud computing jako datové uložiště, dále pak pro práci nad sdílenými dokumenty.

Pátá kapitola se věnovala návrhům doporučení pro hrozby, které byly studenty a vysokými veřejnými školami vybrány. Mezi tyto hrozby se řadí nevyžádaná elektronická pošta, porucha hardware, chyba uživatele, selhání LAN a selhání programového vybavení. Část těchto rizik je eliminována právě cloud computingem, jelikož při využívání cloud computingové technologie na sebe určité hrozby přebírá poskytovatel této technologie.

Osobně považuji cloud computingové technologie v procesu vzdělávání za velmi přínosné. Odpadává jakákoliv starost o programové vybavení a aktualizace. Dále jako přínos považuji dostupnost, možnost sdílení dokumentu s více lidmi a pracovat tak v týmu.

Seznam použité literatury

Odborná literatura

RHODES-OUSLEY, Mark. Information Security:The Complete Reference. 2nd ed. New York: McGraw Hill, 2012.896 p. ISBN 978-007-1784-351.

ONDRÁK, Viktor, Petr SLÁDEK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. 377 s. ISBN 978-80-7204-872-4.

DOUCEK, Petr et al. Řízení bezpečnosti informací. 2. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.

KNÝ, Milan a Josef POŽÁR. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno: Tribun EU, 2010. 128 s. Knihovnicka.cz. ISBN 978-80-7399-067-1.

RODRYČOVÁ, Danuše. Bezpečnost informací jako podmínka prosperity firmy. 1.vyd. Praha: Grada Publishing, 2000. 143 s. ISBN 80-716-9144-5.

PAVLÍČEK, Antonín. Nová média a sociální sítě. Vyd. 1. Praha: Oeconomica, 2010. 181 s. ISBN 978-802-4517-421.

Sláma, Michal et al. Průzkum stavu informační bezpečnosti na veřejných vysokých školách v České republice 2012.

SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. 483 s. Expert (Grada). ISBN 978-80-247-4644-9.

Internetové zdroje

ZÍTKO, Jan. Cloud Computing: Jeho výhody a nevýhody?. [online]. [cit. 2015-01-31]. Dostupné z: http://google-apps.cz/co-je-cloud-computing-jeho-vyhody-a-nevyhody-2

ZÍTKO, Jan. Co je „Cloud computing“?. [online]. [cit. 2015-01-31]. Dostupné z: http://www.janzitko.cz/co-je-cloud-computing/

ZIKMUND, Martin. Co je to Cloud computing a proč se o něm mluví. [online]. [cit. 2015-01-31]. Dostupné z:http://www.businessvize.cz/software/co-je-to-cloud-computing-a-proc-se-o-nem-mluvi

CLOUD.CZ. Cloud computing: Co ty pojmy znamenají [online]. Cloud[online]. [cit.2015-01-31]. Dostupné z: http://www.cloud.cz/cloud/158-cloud-computingco-ty-pojmy-znamenaji.html

MÁCHA, Petr. Cloud computing – historie a budoucnost: Historie CLOUD computingu. [online]. [cit. 2015-02-01]. Dostupné z:http://www.ddconnect.cz/brezen-2012/datova-centra.html

ZIVE.CZ. Cloud computing: Za minutu dvanáct [online]. [cit. 2015-02-01]. Dostupné z: http://www.zive.cz/clanky/cloud-computing-za-minutu-dvanact/sc-3-a-157339/

FIELDER, Kevin. Very simple Introduction to Cloud Computing: Just what is Cloud computing? [online]. [cit. 2015-02-01]. Dostupné z: https://kevinfielder.wordpress.com/2012/06/21/very-simple-introduction-to-cloud-computing/

LEJSEK, Zdeněk. SYSTEMONLINE. Nové přístupy k bezpečnosti cloudu [online]. [cit. 2015-02-04]. Dostupné z:http://www.systemonline.cz/virtualizace/nove-pristupy-k-bezpecnosti-cloudu.htm

CHLUP, Marek. ČESKÝ INSTITUT MANAŽERŮ INFORMAČNÍ BEZPEČNOSTI. Bezpečnost ICT. [online]. s. 43 [cit. 2015-02-05]. Dostupné z: http://www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf

ŠMÍD, Vladimír. Pojem informačního systému [online]. [cit. 2015-02-05]. Dostupné z: http://www.fi.muni.cz/~smid/mis-infsys.htm

Úplné znění zákona č. 412/2005. In: O ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. 2005. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005

Předpis č. 101/2000 Sb. In: Zákon o ochraně osobních údajů a o změně některých zákonů. 2000. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-101

Zákon č. 227/2000. In: O elektronickém podpisu. 2000. Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

Zákon č. 365/2000. In: O informačních systémech veřejné správy. 2000. Dostupné z: http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

KNOTEK, Martin. DS5 Zabezpečení systémové bezpečnosti. [online]. [cit. 2015-03-03]. Dostupné z:http://blog.vyvojar.cz/dotnet/archive/2012/07/27/243300.aspx

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI a NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Zpráva o stavu kybernetické bezpečnosti České republiky: Výroční zpráva Národního centra kybernetické bezpečnosti podle usnesení vlády ze dne 19. října 2011 č. 781. [online]. [cit. 2015-03-12]. Dostupné z: www.govcert.cz/download/nodeid-598

NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti: Information security management system [online]. [cit. 2015-03-12]. Dostupné z: http://www.cybersecurity.cz/data/srib.pdf

WIRNITZEROVÁ. Co si učitelé myslí o mobilních technologiích?: Rizika mobilních technologii. [online]. 2013 [cit. 2015-04-09]. Dostupné z:http://spomocnik.rvp.cz/clanek/18147/CO-SI-UCITELE-MYSLI-O-MOBILNICH-TECHNOLOGIICH.html

CLOUD.CZ. Sedm rizik cloud computingu [online]. [cit. 2015-04-10]. Dostupné z: http://www.cloud.cz/bezpenost/84-gartner-sedm-rizik-cloud-computingu.html

LOUŽECKÁ, Iva. 10 důvodů proč využívat Cloudu ve vzdělávání. [online]. [cit. 2015-04-10]. Dostupné z:http://www.veskole.cz/clanky/10-duvodu-proc-vyuzivat-cloudu-ve-vzdelavani

TVRDÍKOVÁ, Milena. Zkušenosti s využitím Cloud Computingu ve vzdělávání, In: Vimeo [online]. Zveřejněno 12. 04. 2015 [vid. 2013-03-21]. Dostupné z: https://vimeo.com/62687272

KOLAJA, Marcel a Miroslav BARTOŠEK. Jemný úvod do (anti)spamové problematiky: Obrana proti spamu. [online]. [cit. 2015-04-14]. Dostupné z: http://ics.muni.cz/bulletin/articles/251.html#back6

ŘEHÁK, David. Úvod do problematiky řízení rizik. [online]. [cit. 2015-04-14]. Dostupné z:http://www.researchgate.net/publication/261437852_vod_do_problematiky_zen_rizik

DONÁT, Josef. SystemOnLine: S přehledem ve světě informačních technologií: Právní aspekty cloud computingu. [online]. 2011 [cit. 2015-04-17]. Dostupné z: http://www.systemonline.cz/virtualizace/pravni-aspekty-cloud-computingu.htm.

ISO Normy

ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systém – Requirements.

ČNS ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2010.

ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2009

ČNS ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2005.

ČNS ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006.

Seznam zkratek

AI	-	Artificial Intelligence
CaaS	-	Communication as a Service
CRM	-	Customer Relationship Management
ČNS	-	Česká technická norma
EDISON	-	Education Information Systém on Net
GNU	-	GNU's Not Unix
IaaS	-	Infrastructure as a Service
ICT	-	Information and Communication Technology
IEC	-	International Electrotechnical Commission
IS	-	Information System
ISMS	-	Information Security Management System
ISO	-	International Organization for Standardization
IT	-	Information Technology
ITIL	-	Information Technology Infrastructure Library
LAN	-	Local Area Network
MSP	-	Managed Service Provides
NBÚ	-	Národní bezpečnostní úřad
PaaS	-	Platform as a Service
PDCA	-	Plan-Do-Check-Act
PIN	-	Personal Identification Number
PKI	-	Public Key Infrastructure
SaaS	-	Software as a Service
SMS	-	Short Message Service
UPS	-	Uninterruptible Powerr Supply
URL	-	Uniform Resource Locator

USB	-	Universal Serial Bus
VLAN	-	Virtual Local Area Networks
VŠB-TUO	-	Vysoká škola báňská - Technická univerzita Ostrava

Seznam obrázků

Seznam grafů

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 25. 4. 2015

Bc. Andrea Owczarzová

Seznam příloh

Příloha č. 1 : Dotazník

Upravit formulář

Řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na Vysoké škole báňské – Technické univerzitě Ostrava

Tento průzkum je součástí diplomové práce na téma řízení a zvládání rizik na VŠB-TU a řízení a zvládání rizik v Cloud computingovém prostředí na VŠB-TU Ostrava.

*Povinné pole

Víte co pojem Cloud computing znamená? *

- ○ Už jsem o tom slyšel/a
- ○ Tento pojem slyším poprvé
- ○ Tento pojem znám velmi dobře a přesně vím, co znamená

Jaké kancelářské balíky aplikací používáte? *

- ☐ MS Office
- ☐ MS Office 365
- ☐ Google Apps
- ☐ Open Office
- ☐ Jiné

Využíváte on-line řešení pro tvorbu školních dokumentů? *
Sdílení dokumentu na internetu s možností úprav jinými uživateli

- ○ Ano
- ○ Ne

Dávám přednost službám *

- ○ Obecně placeným
- ○ Připlatím si rád za řešení od firmy, kterou preferuji.
- ○ Obecně zdarma
- ○ Cloudové služby nepoužívám

Citlivá data svěřená mimo vlastní uložiště jsou: *

- ○ Zcela v bezpečí, klidně data svěřím poskytovatelům Cloudových technologí
- ○ Nedostatečně chráněna, citlivá data poskytovatelům nikdy nesvěřím
- ○ Nevím

Máte obavy ze zneužití svých dat? *
Jedná se o obavy zneužití dat uložených prostřednictvím Cloudu

- ○ Mám
- ○ Mám, přesto používám
- ○ Mám a nepoužívám
- ○ Nemám a používám
- ○ Nepoužívám z jiného důvodu

Jakou z následujících služeb využíváte? *

- ☐ Dropbox
- ☐ OneDrive
- ☐ Disk Google
- ☐ MEGA
- ☐ Žádné
- ☐ Jiné:

V čem shledáváte výhody/nevýhody Cloud computigu?

Pokračovat »

20% dokončeno

Upravit formulář

Řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na Vysoké škole báňské – Technické univerzitě Ostrava

*Povinné pole

Využívání Cloudových technologií na VŠB-TU Ostrava

Využíváte ve škole nějaké on-line uložiště dat v Internetu? *
Např. SkyDrive, GoogleDrive, uschovna.cz, ulozto.cz

- Ano
- Ne

Používá se na škole sdílení dokumentů, jako forma distribuce materiálů pro studenty? *
Například vystavované přednášky, materiály na hodiny, které si studenti mohou stáhnout.

- Ano
- Ne

Jaký typ služeb si myslíte, že škola používá?*

- Saas
- PaaS
- IaaS
- Žádné
- Nevím
- Jiné

Víte, jaké jsou roční náklady školy na kancelářský software? *

- Nevím
- Používáme řešení zdarma / škola má sponzora
- 1 - 1000 CZK
- 1001 - 10 000 CZK
- více než 10 000 CZK

Víte, jaké jsou roční náklady školy na správu uložených dat?

- Nevím
- Používáme řešení zdarma / škola má sponzora
- 1 - 1000 CZK
- 1001 - 10 000 CZK
- více než 10 000 CZK

Upravit formulář

Řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na Vysoké škole báňské – Technické univerzitě Ostrava

*Povinné pole

Portál lms.vsb.cz

Využíváte portál lms.vsb.cz jako učební pomůcku? *

- Ano
- Spíše ano
- Spíše ne
- Ne

Jsou materiály na portálu dostačující?

- Ano
- Spíše ano
- Spíše ne
- Ne

Jak hodnotíte kvalitu materiálů, které jsou na portálu ke stažení?
Známkování jako ve škole, 1 - nejlepší, 5 - nejhorší

- 1
- 2
- 3
- 4
- 5

Jakou didaktickou pomůcku byste nejvíce uvítali v e-learningu? *

- Videokonference
- Online chat
- Videozáznamy
- Tištěné materiály

« Zpět Pokračovat »

60% dokončeno

Upravit formulář

Řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na Vysoké škole báňské – Technické univerzitě Ostrava

*Povinné pole

Řízení a zvládání rizik

Které z těchto oblastí považujete v rámci VŠB-TU za největší výzvu z hlediska bezpečnosti? *

- [ ] Virtualizace desktopů
- [ ] Integrace logické a fyzické bezpečnosti
- [ ] Kryptování disků
- [ ] Kryptování emailů
- [ ] Změna SW platformy
- [ ] Bezdrátové služby (wifi)
- [ ] Webové aplikace
- [ ] Digital Rights Management
- [ ] Mobilní komunikace (PDA, smart phones)
- [ ] Elektronická komunikace (instant messaging, email)
- [ ] Teleworking
- [ ] Voice-over-IP (VoIP)
- [ ] Virtualizace serverů
- [ ] Přenosná média (např. USB flash disky)
- [ ] Radio Frequency Identifiers (RFID)

Vyberte prosím 3 hlavní překážky, jenž si myslíte, že brání rychlejšímu prosazování informační bezpečnosti na VŠB-TU. *

- [ ] Nedostatečná a nevyvážená legislativa ČR
- [ ] Obecně nízké bezpečnostní vědomí
- [ ] Finanční náročnost
- [ ] Nedostatečná podpora ze strany vedení organizace
- [ ] Neexistence českého bezpečnostního standardu
- [ ] Nezájem a nekompetentnost státních orgánů
- [ ] Nedostatek informací
- [ ] Technologická náročnost
- [ ] Nedostatek tuzemských expertů
- [ ] Jiný důvod

Které bezpečnostní incidenty proběhly dle Vás na VŠB-TU? *

- [ ] Nevyžádaná elektronická pošta (SPAM)
- [ ] Výpadek proudu
- [ ] Porucha hardware
- [ ] Chyba uživatele
- [ ] Počítačový virus
- [ ] Chyba programového vybavení
- [ ] Selhání LAN
- [ ] Chyba administrátora nebo obsluhy
- [ ] Krádež zařízení
- [ ] Nepovolený přístup k datům – zevnitř
- [ ] Zneužití zařízení
- [ ] Přírodní katastrofa
- [ ] Selhání WAN
- [ ] Únik informací
- [ ] Nepovolený přístup k datům – zvenčí
- [ ] Falšování elektronických dokumentů, transakcí a informací

Myslíte si, že má VŠB-TU vypracované a připravené plány obnovy funkčnosti informačního systému? *

- ( ) Ano
- ( ) Ne

Pokud ano, tak myslíte si že jsou tyto plány testovány pravidelně?

- ( ) Ne
- ( ) Ano, alespoň jednou za rok
- ( ) Ano, alespoň jednou za dva roky
- ( ) Ano, ale v delším intervalu než jednou za dva roky

« Zpět Pokračovat »

80% dokončeno

Upravit formulář

Řízení a zvládání rizik vyplývajících z bezpečnostních hrozeb na Vysoké škole báňské – Technické univerzitě Ostrava

*Povinné pole

Osobní data respondentů

Pohlaví *

- Žena
- Muž

Věk *

- 18 - 20
- 21 - 23
- 24 - 26
- 27 a více

Jsem studentem na *

- HGF (Hornicko-geologická fakulta)
- FMMI (Fakulta metalurgie a materiálového inženýrství)
- FS (Fakulta strojní)
- EKF (Ekonomická fakulta)
- FEI (Fakulta elektrotechniky a informatiky)
- FAST (Fakulta stavební)
- FBI (Fakulta bezpečnostního inženýrství)

« Zpět Odeslat

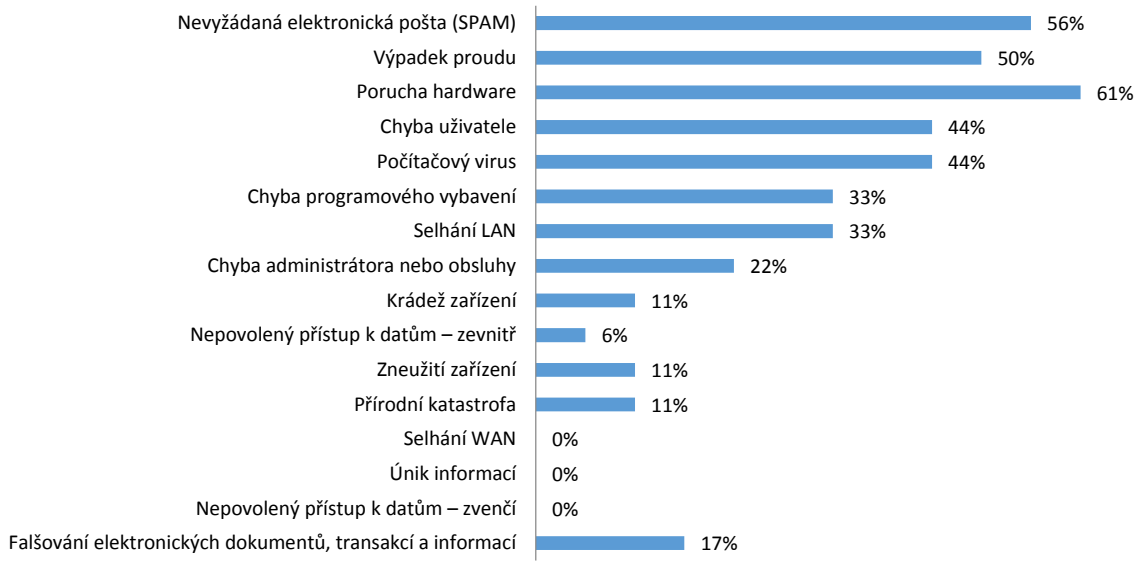
100 %: Hotovo.

Nikdy přes Formuláře Google neposílejte hesla.

Příloha č. 2 : Vyhodnocení průzkumu

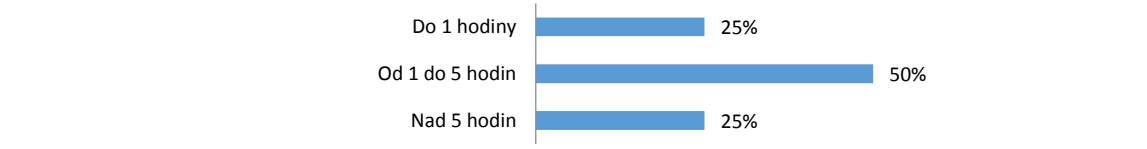
ŘÍZENÍ A ZVLÁDÁNÍ RIZIK

Žádná rizika by neměla být podceňována. V průběhu posledních dvou let musely téměř všechny vysoké školy čelit bezpečnostním incidentům, což potvrzuje význam informační bezpečnosti a potřebu zaměření se na tuto oblast. Nejčastěji zaznamenaným bezpečnostním incidentem je porucha hardware.



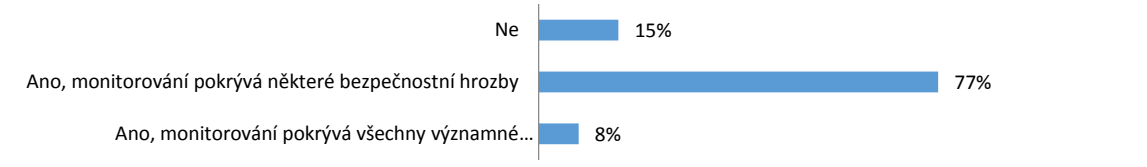
Graf 1: Bezpečnostní incidenty zaznamenané v rámci vysokých škol za poslední dva roky

Rychlost detekce bezpečnostního incidentu může významně ovlivnit náklady na jeho řešení. Největší podíl respondentů uvedl, že na jejich univerzitě byli schopni detekovat bezpečnostní incident od 1 – 5 hodin. Přibližně 25 % univerzit pak zaznamenalo bezpečnostní incident po více než 5 hodinách. Většina respondentů je tedy schopna v relativně krátkém čase detekovat bezpečnostní incidenty, byť v některých případech nemusí být schopnost detekce bezpečnostních incidentů do 5 hodin dostačující. Zároveň schopnost detekce bezpečnostních incidentů prokazuje, že většina univerzit má zavedeno monitorování těchto incidentů, což potvrzují výsledky uvedené v grafu č. 3.



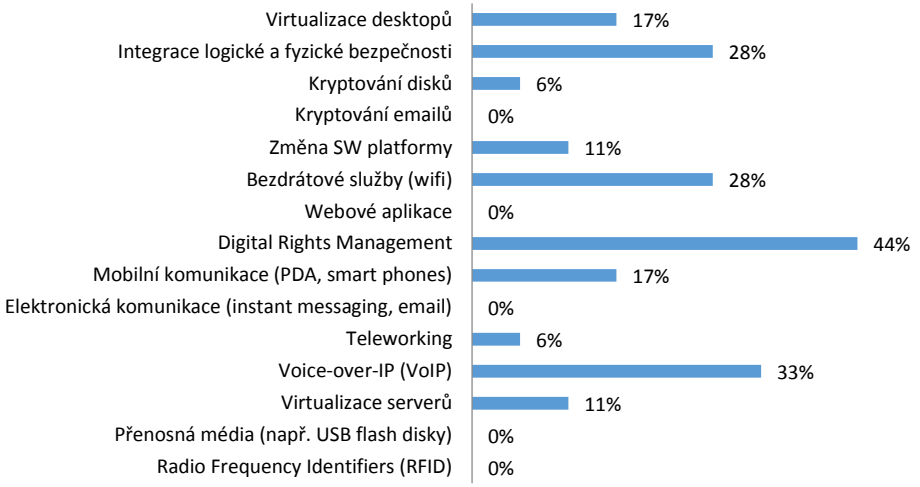
Graf 2: Jak rychle jste byli schopni detekovat bezpečnostní incidenty od okamžiku jejich zachycení?

Systém monitorování bezpečnostních hrozeb má alespoň z části zavedeno přes 80 % univerzit, což je poměrně dobrý výsledek.



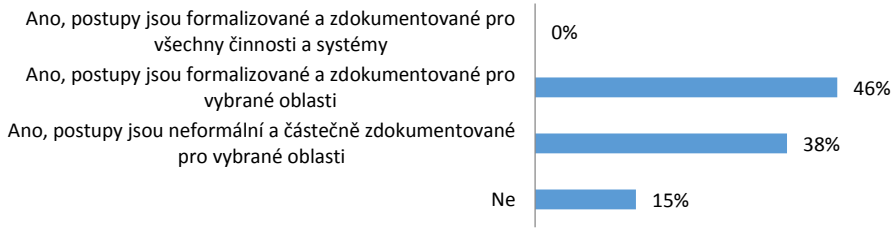
Graf 3: Máte zaveden systém monitorování bezpečnostních incidentů?

Největší výzvou z hlediska bezpečnosti je pro většinu respondentů Digital Rights Management, Voice-over-IP (VoIP), integrace logické a fyzické bezpečnosti a bezdrátové služby (WIFI).



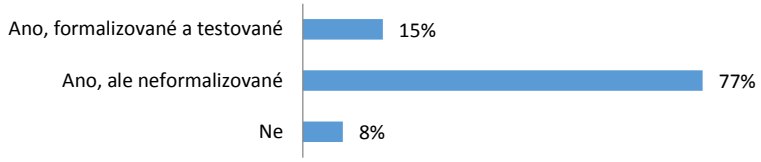
Graf 4: Které z těchto oblastí považujete v rámci Vaší vysoké školy za největší výzvu z hlediska bezpečnosti?

Jasně definované postupy pro případ výskytu bezpečnostního incidentu zajišťují včasné a efektivní řešení vzniklé nežádoucí situace a minimalizují možné následky. Téměř polovina respondentů uvedla, že na jejich vysoké škole tyto formalizované postupy existují alespoň pro vybrané rizikové oblasti. V návaznosti na výsledky uvedené v grafu č. 3 je tedy možno odvodit, že má-li univerzita zavedeno monitorování bezpečnostních incidentů, má alespoň pro vybrané typy bezpečnostních incidentů připraven postup jejich řešení.



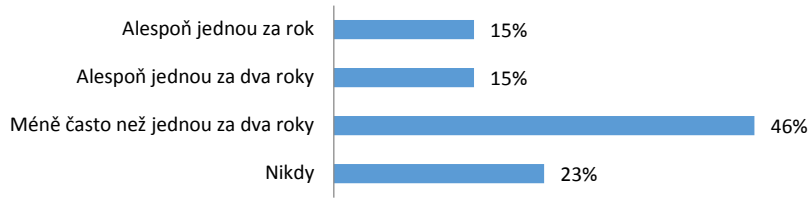
Graf 5: Máte definovány postupy reakce na výskyt bezpečnostních incidentů?

Plány obnovy funkčnosti systému hrají v oblasti řízení informační bezpečnosti důležitou roli. Majoritní podíl respondentů uvádí, že jejich univerzita má vypracované plány obnovy, ve většině případů ovšem nejsou formalizované.



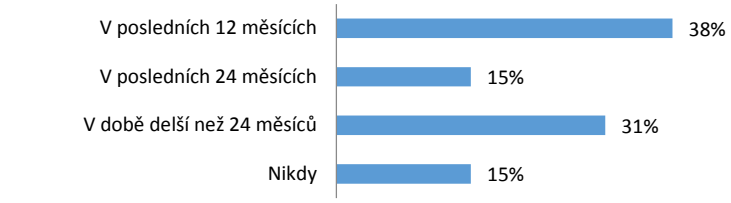
Graf 6: Má Vaše vysoká škola/univerzita vypracované a připravené plány obnovy funkčnosti informačního systému?

Testování umožňuje prověřit funkčnost plánů obnovy a jejich možné nedostatky. Pokud tedy plány nikdy testovány nebyly, lze předpokládat, že mohou být neúčinné. Z výsledku průzkumu vyplývá, že v univerzitním prostředí převažuje podíl respondentů, kteří své plány obnovy testují v intervalu delším než 2 roky. Další významná část respondentů pak nikdy plány obnovy neprověřila.



Graf 7: Jsou tyto plány obnovy pravidelně testovány?

Analýza rizik představuje základ systému řízení informační bezpečnosti. Bez výsledků analýzy rizik je velice obtížné určit, jaké hrozby jsou skutečně relevantní a jaký mohou mít dopad. Vysoký počet univerzit dosud neprovádí pravidelně analýzu rizik. Následně pak 15% respondentů pak uvádí, že analýzu rizik na jejich univerzitě nerealizovali nikdy.

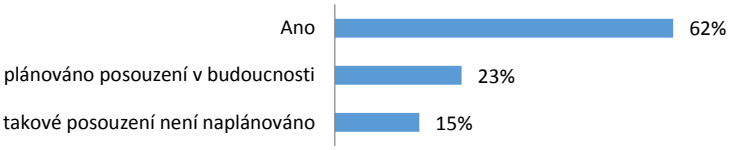


Graf 8: Kdy naposledy byla na Vaší škole provedena analýza rizik IS?

Více než polovina vysokých škol řeší bezpečnost svých aktiv ve spolupráci s externími firmami. Přibližně třetina škol pak zajišťuje informační bezpečnost výhradně vlastními silami.

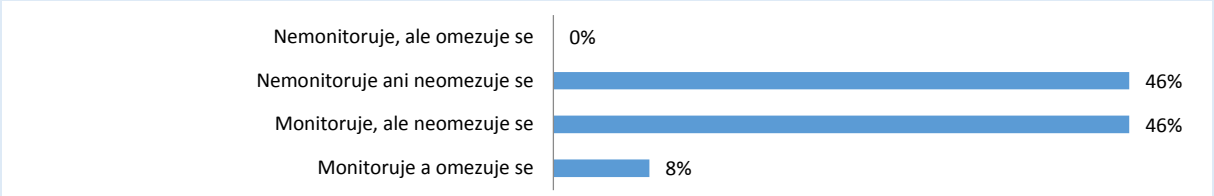
Graf 9: Jakým způsobem řešíte informační bezpečnost na Vaší vysoké škole?

Naprostá většina vysokých škol již má posouzenu oblast informační bezpečnosti externím subjektem nebo toto posouzení plánuje v budoucnu. Zde je patrné, že informační bezpečnost je pro univerzitní prostředí významným faktorem.



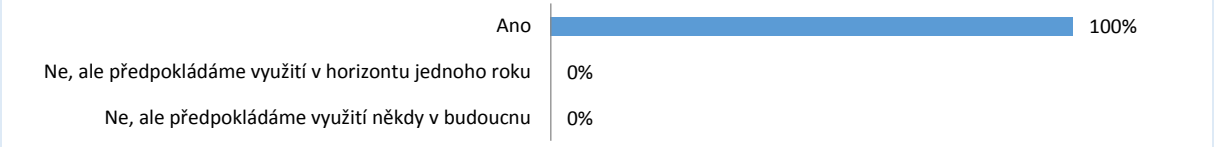
Graf 10: Byla oblast informační bezpečnosti posouzena externím subjektem (např. audit nebo bezpečnostní certifikace)?

Přibližně 46% respondentů uvedlo, že své zaměstnance nemonitoruje a ani neomezuje. Následně stejný podíl respondentů odpovědělo, že své zaměstnance monitoruje, ale taktéž neomezuje. Celkově své zaměstnance omezuje 8% respondentů.



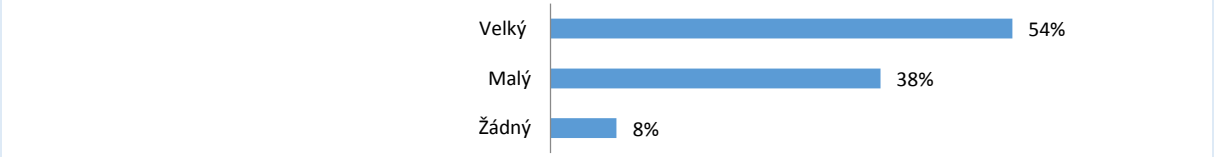
Graf 11: Monitoruje anebo omezuje se používání internetu zaměstnanci univerzity?

Na vysokých školách je elektronický podpis využíván poměrně často. Všichni respondenti, kteří na otázku odpověděli, uvedli, že elektronický podpis používají.



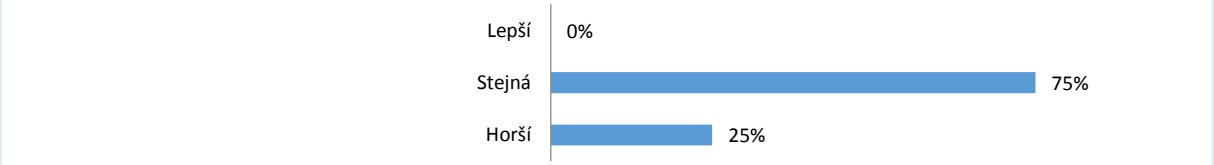
Graf 12: Využíváte na Vaší vysoké škole v rámci svých činností elektronický podpis?

Většina respondentů uvedla, že dopad zákona o ochraně osobních údajů na řešení informační bezpečnosti v rámci jejich vysoké školy je značný.



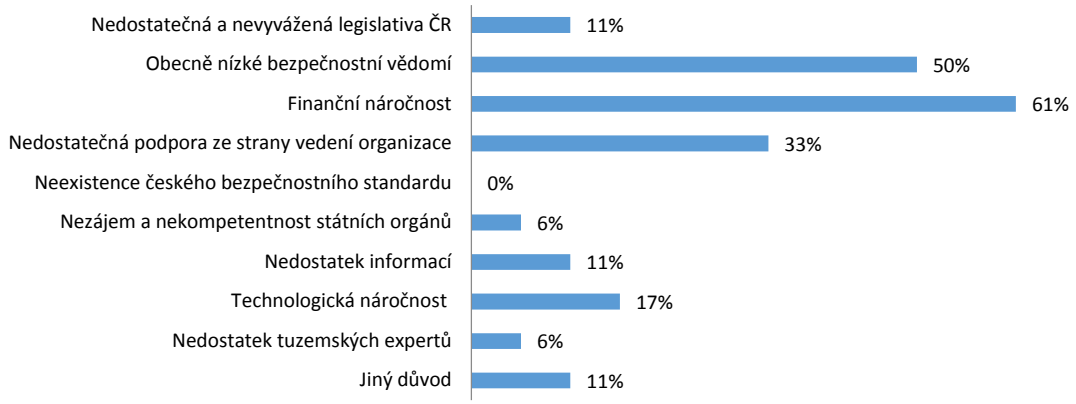
Graf 13 Jaký je vliv zákona o ochraně osobních údajů na informační bezpečnost Vaší vysoké školy?

Úroveň informační bezpečnosti na vysokých školách v České republice hodnotila více než polovina respondentů jako srovnatelnou ve vztahu k západoevropským státům.



Graf 14 Jak hodnotíte úroveň informační bezpečnosti na vysokých školách v ČR ve vztahu k západoevropským státům?

Za největší překážky prosazování informační bezpečnosti jsou považovány finanční náročnost, obecně nízké bezpečnostní povědomí a nedostatečná podpora ze strany vedení organizace.



Graf 15: Hlavní překážky rychlejšího prosazování informační bezpečnosti na vysokých školách v ČR